On the structure of Witt-Burnside rings attached to pro-p groups

Lance Edward Miller

1 Introduction

Classical Witt vectors are a functorial construction that takes perfect fields k of characteristic p to domains $\mathbf{W}(k)$ of characteristic 0 with residue field k. This is surprising, as most functorial operations in algebra take rings of characteristic p to other rings of characteristic p. For a perfect field k of characteristic $p > 0$, the ring of classical Witt vectors $\mathbf{W}(k)$ is a minimal example of a complete discrete valuation ring unramified at p with residue field k. These are of interest in number theory [9], Galois theory [5, 14], algebraic groups [10] and Fontaine rings [13].

The construction of the classical Witt vectors uses the Witt polynomials to define certain addition and multiplication polynomials with rational coefficients which do not obviously have integral coefficients. A. Dress and C. Siebeneicher generalized the Witt polynomials to a family of multivariable polynomials associated to any profinite group G [1]. Like classical Witt polynomials, these polynomials obviously have $\mathbf{Q}$-coefficients and a significant theorem of Dress and Siebeneicher shows that they in fact have integral coefficients. Thus one can use these polynomials, in an analogous way to the construction of classical Witt vectors, to define a functor $\mathbf{W}_G$ on the category of commutative rings for each profinite group G. For infinite pro-p groups G, the ring $\mathbf{W}_G$ retains the surprising property of taking rings of characteristic p to rings of characteristic 0.

The rings $\mathbf{W}_G$ are called Witt-Burnside rings since when $G = \mathbf{Z}_p$ the ring $\mathbf{W}_G(A)$ is the classical (p-typical) Witt vectors of A, and when G is arbitrary $\mathbf{W}_G(\mathbf{Z})$ is the Burnside ring of G. This interpretation of $\mathbf{W}_G(\mathbf{Z})$ was a motivation for Dress and Siebeneicher's construction of the functor $\mathbf{W}_G$ in general.

The classical Witt vectors are recovered by the choice $G = \mathbf{Z}_p$ and Cartier's "big" Witt vectors correspond to the choice $G = \widehat{\mathbf{Z}}$. The name Burnside appears as for any profinite group G, $\mathbf{W}_G(\mathbf{Z})$ is the Burnside ring of G. This was a large part of what initiated the study of these functors. Others constructions of these functors have been studied. Specifically, J. Graham constructs Witt-Burnside rings using ring valued G-sets [2]. J. Elliott gave an unified construction relating the Graham and Dress and Siebeneicher approaches [4]. Y. Oh has studied some decomposition and q-deformation questions [7, 8]. Beyond the classical $G = \mathbf{Z}_p$ case, not much about the ring structure of $\mathbf{W}_G(k)$ is known. Motivated by the extensive applications enjoyed by the classic Witt vectors, this paper addresses structural questions about Witt-Burnside rings under the assumptions that G is an infinite pro-p group and k is a field of characteristic $p > 0$.

For perfect fields of characteristic p, $\mathbf{W}_{\mathbf{Z}_p}(k)$ is the ring of classical Witt vectors; a p-adically complete discrete valuation domain with maximal ideal (p) and residue field k. For infinite pro-p $G \not\cong \mathbf{Z}_p$, we will show that the ring $\mathbf{W}_G(k)$ is also a local ring of characteristic 0 (Corollary 3.21) however, the similarities do not run deep!

Theorem *For $G = \mathbf{Z}_p^d$, k a field of characteristic $p > 0$ and $d \geq 2$, the maximal ideal of $\mathbf{W}_G(k)$ is not finitely generated, so $\mathbf{W}_G(k)$ is not Noetherian.*

The next motivating question is whether the rings $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ are coherent for a field of characteristic p. A necessary condition for coherence is that all annihilator ideals are finitely generated [3, p. 95]. We show this condition also fails for $\mathbf{W}_G(k)$ for $G = \mathbf{Z}_p^d$ and $d \geq 2$ indicating that these rings are much larger than expected.

While it essentially follows from [1] that $\mathbf{W}_G(k)$ is not a domain in general, our second main goal is to give some control on the zero divisors of $\mathbf{W}_G(k)$ for $G = \mathbf{Z}_p^2$ and k a field of characteristic p.

Theorem *For $G = \mathbf{Z}_p^2$ and any field k of characteristic p, the ring $\mathbf{W}_G(k)$ is reduced.*

While we suspect $\mathbf{W}_G(k)$ is reduced for $G = \mathbf{Z}_p^d$ for $d \geq 2$ and any field K of characteristic p, the methods used here fail for $d > 2$ due to the reliance on a certain property of the subgroup structure of $\mathbf{Z}_p^2$. In Section 6 we describe a natural family of non-maximal prime ideals in $\mathbf{W}_{\mathbf{Z}_p^d}(k)$, and from this theorem we will know that our list of non-maximal prime ideals is not complete when $d = 2$.

The rest of the paper is organized as follows. Section 2 will develop the preliminary definitions and facts about Witt-Burnside rings, their constructions and their natural profinite topology. Section 3 will discuss other natural topologies on $\mathbf{W}_G(k)$ for pro-p G which align with the familiar topology when $G = \mathbf{Z}_p$, and we will see how they are different in the more general setting. Section 4 will discuss in detail the frame of $\mathbf{Z}_p^d$ for $d \geq 2$; these groups form the basic examples of the paper. Section 5 discusses the failure of finite generation in the maximal ideal and certain annihilator ideals of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ for $d \geq 2$ when the characteristic of k is p. Finally, Section 6 will discuss the kinds of zerodivisors that can occur in $\mathbf{W}_G(k)$. Unless otherwise stated, G will always be a profinite group.

2 Preliminaries

Witt-Burnside rings are constructed utilizing generalized Witt polynomials associated to a profinite group G. The index set of these generalized polynomials is the set of isomorphism classes of discrete finite transitive G-sets, called the *frame* of G and denoted $\mathcal{F}(G)$. For example, $\mathcal{F}(\mathbf{Z}_p) = \mathbf{N}$ by the correspondence $\mathbf{Z}_p/p^n\mathbf{Z}_p \leftrightarrow n$. There is a natural partial ordering on $\mathcal{F}(G)$. For T and U in $\mathcal{F}(G)$ we say $U \leq T$ if there is a G-map from T to U. Denote the set of all G-maps from T to U as $\mathrm{Map}_G(T,U)$ and the number of G-maps $\#\mathrm{Map}_G(T,U)$ by $\varphi_T(U)$. Thus $\varphi_T(U) \neq 0$ if and only if $T \leq U$. We summarize some facts about $\mathcal{F}(G)$ which will be proved later (Lemma 3.11).

1. For T and U in $\mathcal{F}(G)$ with $U \leq T$, $\#U$ divides $\#T$ and $\#T/\#U$ represents the size of any of the fibers of any element of $\mathrm{Map}_G(T,U)$.

2. If the stabilizer subgroups of the points in T are all equal (we will say in this case that T has normal stabilizers or that T is a normal G-set), then $\varphi_T(U) = \#U$ for $U \leq T$.

3. For each T in $\mathcal{F}(G)$, there are only finitely many U in $\mathcal{F}(G)$ with $U \leq T$.

The elements of $\mathcal{F}(G)$ have a concrete description. Every finite transitive G-set T is isomorphic to some coset space G/H with left G-action, where H is an open subgroup of G that can be chosen as the stabilizer subgroup of any point in T. The partial order $\leq$ on coset spaces (considered as G-sets up to isomorphism) can be described concretely by $G/K \leq G/H$ if and only if H is conjugate to a subgroup of K (or equivalently, H is a subgroup of a conjugate of K).

For $T \in \mathcal{F}(G)$, define the T-th *Witt polynomial* to be

$$W_T(\{X_U\}_{U\in\mathcal{F}(G)}) = \sum_{U\leq T} \varphi_T(U) X_U^{\#T/\#U} = X_0^{\#T} + \ldots + \varphi_T(T)X_T, \tag{1}$$

where 0 denotes the trivial G-set G/G. Trivially $\varphi_T(0) = 1$ for all T in $\mathcal{F}(G)$. This is a finite sum since there are only finitely many $U \leq T$.

For instance, if $G = \mathbf{Z}_p$ then the finite transitive G-sets up to isomorphism are $\mathbf{Z}_p/p^n\mathbf{Z}_p$ for $n \geq 0$ and the Witt polynomial associated to $\mathbf{Z}_p/p^n\mathbf{Z}_p$ is the classical n-th Witt polynomial. Figure 1 displays the frame of $\mathbf{Z}_2^2$. When $G = \mathbf{Z}_p^2$, all G-sets have $p+1$ covers (that is, there are exactly $p+1$ G-sets in the frame lying immediately above each G-set). Other than the trivial G-set, each G-set below the lowest horizontal line in Figure 1 has p covers also below the lowest horizontal line.

Remark 2.1. The picture in Figure 1 is reminiscent of the tree of $\mathbf{Z}_2$-lattices in $\mathbf{Q}_2^2$ up to scaling, on which $\mathrm{PGL}_2(\mathbf{Q}_2)$ acts [11, p. 71]. However, it is different since the G-sets $\mathbf{Z}_2^2/2^r\mathbf{Z}_2^2$ appear as separate vertices in Figure 1, while the subgroups $2^r\mathbf{Z}_2^2$ all correspond to the same vertex in the tree for $\mathrm{PGL}_2(\mathbf{Q}_2)$.

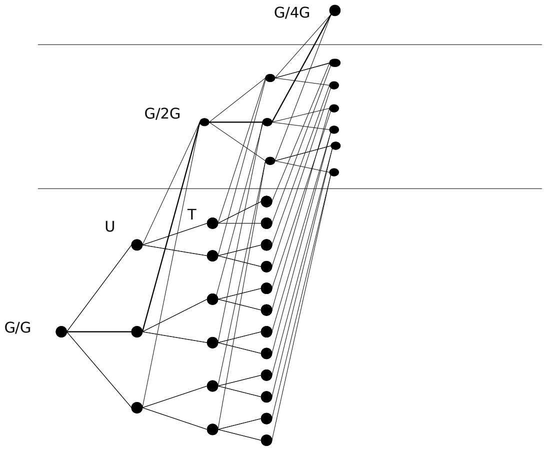

Figure 1: The frame $\mathcal{F}(\mathbf{Z}_2^2)$.

To simplify notation, write a tuple of variables X_T indexed by all T in $\mathcal{F}(G)$ as $\underline{X}$, e.g., $W_T(\{X_U\}_{U\in\mathcal{F}(G)}) = W_T(\underline{X})$, $\mathbf{Z}[\{X_T\}_{T\in\mathcal{F}(G)}] = \mathbf{Z}[\underline{X}]$, and $\mathbf{Z}[\{X_T, Y_T\}_{T\in\mathcal{F}(G)}] = \mathbf{Z}[\underline{X}, \underline{Y}]$. This underline notation of course depends on G. For any commutative ring A, a polynomial $f(\underline{X}) \in \mathbf{Z}[\underline{X}]$ defines a function from $\prod_{T\in\mathcal{F}(G)} A$ to A, and for a tuple $\mathbf{a} = (a_T)_{T\in\mathcal{F}(G)}$ with coordinates in A we write $f(\mathbf{a}) = f(\{a_T\}_{T\in\mathcal{F}(G)}) \in A$. A similar meaning is applied to $f(\mathbf{a}, \mathbf{b})$ for a polynomial $f(\underline{X}, \underline{Y}) \in \mathbf{Z}[\underline{X}, \underline{Y}]$. Generally we write sequences indexed by $\mathcal{F}(G)$ as bold letters (*e.g.*, $\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}, \mathbf{v}$) and their T-th coordinate is in italics (*e.g.*, a_T, b_T, x_T, y_T, v_T).

Because X_T appears on the right side of (1) just in the linear term $\varphi_T(T)X_T$, and all variables which appear in other terms are X_U for $U < T$, we get the following uniqueness criterion for all the Witt polynomial values together which is equivalent to Lemma 2.1 in [4, p. 331].

Theorem 2.2. *If A is a commutative ring which has no $\varphi_T(T)$-torsion, then the function $\prod_{T\in\mathcal{F}(G)} A \to \prod_{T\in\mathcal{F}(G)} A$ given by $\mathbf{a} \mapsto (W_T(\mathbf{a}))_{T\in\mathcal{F}(G)}$ is injective. This function is bijective provided each $\varphi_T(T)$ is a unit in A.*

Proof. Suppose $W_T(\mathbf{a}) = W_T(\mathbf{b})$ for all T. We want to show $\mathbf{a} = \mathbf{b}$, i.e., $a_T = b_T$ for all T. This will be done by induction on $\#T$. The only T with $\#T = 1$ is the trivial G-set $0 = G/G$, and $W_0(\mathbf{a}) = a_0$ and $W_0(\mathbf{b}) = b_0$, so $a_0 = b_0$.

For some $n > 1$ assume $a_U = b_U$ for all U with $\#U < n$. If $\#T = n$, write the equation $W_T(\mathbf{a}) = W_T(\mathbf{b})$ as

$$\sum_{U<T} \varphi_T(U) a_U^{\#T/\#U} + \varphi_T(T)a_T = \sum_{U<T} \varphi_T(U) b_U^{\#T/\#U} + \varphi_T(T)b_T.$$

Since $U < T \Rightarrow \#U < \#T$, $a_U = b_U$ for all $U < T$, so we cancel common terms on both sides and get $\varphi_T(T)(a_T - b_T) = 0$. Therefore $a_T - b_T = 0$ by hypothesis, so $a_T = b_T$. □

Corollary 2.3. *Let A be a commutative ring in which every integer $\varphi_T(T)$ is invertible. Then the function $\prod_{T\in\mathcal{F}(G)} A \to \prod_{T\in\mathcal{F}(G)} A$ given by $\mathbf{a} \mapsto (W_T(\mathbf{a}))_{T\in\mathcal{F}(G)}$ is a bijection.*

Proof. This mapping is injective by Theorem 2.2. To prove surjectivity, we choose $\mathbf{b} \in \prod_{T\in\mathcal{F}(G)} A$ and want to construct an $\mathbf{a} \in \prod_{T\in\mathcal{F}(G)} A$ such that $b_T = W_T(\mathbf{a})$ for all T. This will be done recursively based on $\#T$. The point is that the T-th Witt polynomial only depends on variables indexed by $U \leq T$, and if $U < T$ then $\#U < \#T$.

Starting at $\#T = 1$, $T = 0$ and we need $b_0 = W_0(\mathbf{a}) = a_0$, so define $a_0 = b_0$.

For $n > 1$, assume we have found $a_U \in A$ for all U with $\#U < n$ such that $b_T = W_T(\{a_U\}_{U\leq T})$ for all T with $\#T < n$. Then for every T such that $\#T = n$, we want to find an $a_T \in A$ such that

$$b_T = W_T(\{a_U\}_{U\leq T}) = \sum_{U<T} \varphi_T(U) a_U^{\#T/\#U} + \varphi_T(T) a_T.$$

Every term on the right side is already defined except for a_T, and $\varphi_T(T)$ is assumed to be invertible in A, so we can solve for a_T to define it. □

Example 2.4. If G is a pro-p group and $T \cong G/H$, then $\varphi_T(T) = [\mathrm{N}_G(H) : H]$ is a power of p, so if p is invertible in A then every $\mathbf{a} \in \prod_{T\in\mathcal{F}(G)} A$ has the form $(W_T(\mathbf{b}))_{T\in\mathcal{F}(G)}$ for a unique $\mathbf{b} \in \prod_{T\in\mathcal{F}(G)} A$.

The most important application of Theorem 2.2 is to the ring $A = \mathbf{Q}[\underline{X}, \underline{Y}]$ and the vectors $(W_T(\underline{X}) + W_T(\underline{Y}))_{T\in\mathcal{F}(G)}$ and $(W_T(\underline{X})W_T(\underline{Y}))_{T\in\mathcal{F}(G)}$. It tells us there are unique families of polynomials $\{S_T(\underline{X}, \underline{Y})\}$ and $\{M_T(\underline{X}, \underline{Y})\}$ in $\mathbf{Q}[\underline{X}, \underline{Y}]$ satisfying

$$W_T(\underline{X}) + W_T(\underline{Y}) = W_T(\underline{S}) \text{ for all } T \in \mathcal{F}(G)$$

and

$$W_T(\underline{X})W_T(\underline{Y}) = W_T(\underline{M}) \text{ for all } T \in \mathcal{F}(G).$$

More explicitly, this says

$$\sum_{U\leq T} \varphi_T(U) X_U^{\#T/\#U} + \sum_{U\leq T} \varphi_T(U) Y_U^{\#T/\#U} = \sum_{U\leq T} \varphi_T(U) S_U^{\#T/\#U} \tag{2}$$

and

$$\left(\sum_{U\leq T} \varphi_T(U) X_U^{\#T/\#U}\right)\left(\sum_{U\leq T} \varphi_T(U) Y_U^{\#T/\#U}\right) = \sum_{U\leq T} \varphi_T(U) M_U^{\#T/\#U} \tag{3}$$

for all T. The polynomials S_T and M_T each only depend on the variables X_U and Y_U for $U \leq T$.

A significant theorem of Dress and Siebeneicher [1, p. 107], which generalizes Witt's theorem ($G = \mathbf{Z}_p$), says that the polynomials S_T and M_T have coefficients in $\mathbf{Z}$. We call the S_T's and M_T's the Witt addition and multiplication polynomials, respectively. (Obviously they depend on G, but that dependence will not be part of the notation).

Example 2.5. Taking $T = 0$, one has

$$S_0(\underline{X}, \underline{Y}) = X_0 + Y_0 \text{ and } M_0(\underline{X}, \underline{Y}) = X_0 Y_0.$$

If $T \cong G/H$ where H is a maximal open subgroup, so $\{U \leq T\} = \{0, T\}$, solving for S_T and M_T in (2) and (3) yields

$$S_T = X_T + Y_T + \frac{(X_0 + Y_0)^{\#T} - X_0^{\#T} - Y_0^{\#T}}{\varphi_T(T)},$$

$$M_T = X_0^{\#T} Y_T + X_T Y_0^{\#T} + \varphi_T(T) X_T Y_T.$$

Compare with the first two classical Witt addition and multiplication polynomials in [9, p. 42]. Further addition and multiplication polynomials could be very complicated to write out explicitly, as is already apparent for the classical Witt vectors if you try to go past the first two polynomials.

Remark 2.6. If a finite group G contains a maximal subgroup H of index 4 (e.g., $G = A_4$ and $H = A_3$), H can't be a normal subgroup of G since otherwise the G-set $T = G/H$ has $\varphi_T(T) = \#T = 4$ and $((X_0 + Y_0)^4 - X_0^4 - Y_0^4)/4$ doesn't have all integral coefficients. Of course it can be proved by group theory alone that H isn't normal: if $H \lhd G$ then G/H is a group of order 4 and such a group contains a subgroup of order 2, which contradicts maximality of H in G.

Since S_T and M_T have integral coefficients, they can be evaluated on any ring, including rings where the hypotheses of Theorem 2.2 break down, like a ring of characteristic p when G is a pro-p group (Example 3.10).

Definition 2.7. Let G be a profinite group. For any commutative ring A, define the *Witt–Burnside ring* $\mathbf{W}_G(A)$ to be the product space $\prod_{T \in \mathcal{F}(G)} A$ as a set, with elements written as $\mathbf{a} = (a_T)_{T \in \mathcal{F}(G)}$. The ring operations on $\mathbf{W}_G(A)$ are defined using the Witt addition and multiplication polynomials:

$$\mathbf{a} + \mathbf{b} = (S_T(\mathbf{a}, \mathbf{b}))_{T \in \mathcal{F}(G)}$$

and

$$\mathbf{a} \cdot \mathbf{b} = (M_T(\mathbf{a}, \mathbf{b}))_{T \in \mathcal{F}(G)}.$$

The additive (resp. multiplicative) identity is $(0, 0, 0, \dots)$ (resp. $(1, 0, 0, \dots)$).

Even when G is not abelian, $\mathbf{W}_G(A)$ is a commutative ring. For $G = \mathbf{Z}_p$, the addition and multiplication polynomials are the classical Witt addition and multiplication polynomials and $\mathbf{W}_{\mathbf{Z}_p}(A)$ is the p-typical Witt vectors.

To prove that the operations $\oplus$ and $\odot$ put a ring structure on $\mathbf{W}_G(A)$ for any A, it is important that each Witt polynomial W_T is an additive and multiplicative function $\mathbf{W}_G(A) \to A$:

$$\begin{aligned}
W_T(\mathbf{a} \oplus \mathbf{b}) &= \sum_{U \leq T} \varphi_T(U)(\mathbf{a} \oplus \mathbf{b})_U^{\#T/\#U} \\
&= \sum_{U \leq T} \varphi_T(U) S_U(\mathbf{a}, \mathbf{b})^{\#T/\#U} \text{ by the definition of } \oplus \\
&= \sum_{U \leq T} \varphi_T(U)\mathbf{a}_U^{\#T/\#U} + \sum_{U \leq T} \varphi_T(U)\mathbf{b}_U^{\#T/\#U} \text{ by (2)} \\
&= W_T(\mathbf{a}) + W_T(\mathbf{b})
\end{aligned}$$

and similarly

$$W_T(\mathbf{a} \odot \mathbf{b}) = W_T(\mathbf{a})W_T(\mathbf{b}).$$

If we want to prove that $\mathbf{a} \oplus \mathbf{b} = \mathbf{b} \oplus \mathbf{a}$ for all $\mathbf{a}$ and $\mathbf{b}$ in $\mathbf{W}_G(A)$, then observe

$$W_T(\mathbf{a} \oplus \mathbf{b}) = W_T(\mathbf{a}) + W_T(\mathbf{b}) = W_T(\mathbf{b}) + W_T(\mathbf{a}) = W_T(\mathbf{b} \oplus \mathbf{a}) \tag{4}$$

for every T. But this does *not* imply $\mathbf{a} \oplus \mathbf{b} = \mathbf{b} \oplus \mathbf{a}$ because a Witt vector is not necessarily determined by all the Witt polynomials evaluated on it (e.g., if G is a pro-p group and A has characteristic p then $W_T(\mathbf{a}) = a_0^{\#T}$ by Example 3.10, and this only involves a_0 for any T). Theorem 2.2 tells us if two Witt vectors have the same value under all Witt polynomials then the Witt vectors are equal provided the ring A doesn't have too much $\mathbf{Z}$-torsion.

To prove commutativity of addition in $\mathbf{W}_G(A)$, we work in the Witt vectors over a suitable polynomial ring to which Theorem 2.2 applies. We work with the ring $\mathbf{Z}[\underline{X}, \underline{Y}]$ and the specific Witt vectors $\mathbf{x} = (X_T)_{T \in \mathcal{F}(G)}$ and $\mathbf{y} = (Y_T)_{T \in \mathcal{F}(G)}$ in $\mathbf{W}_G(\mathbf{Z}[\underline{X}, \underline{Y}])$. To show

$$\mathbf{x} \oplus \mathbf{y} = \mathbf{y} \oplus \mathbf{x}, \tag{5}$$

it suffices by Theorem 2.2 with $A = \mathbf{Z}[\underline{X}, \underline{Y}]$ to show

$$W_T(\mathbf{x} \oplus \mathbf{y}) = W_T(\mathbf{y} \oplus \mathbf{x}) \text{ for all } T,$$

which is equivalent to showing $W_T(\mathbf{x}) + W_T(\mathbf{y}) = W_T(\mathbf{y}) + W_T(\mathbf{x})$ in $\mathbf{Z}[\underline{X}, \underline{Y}]$ for all T. This is an obvious identity, so (5) is proved. For any T, passing to the T-th coordinate of both sides of (5) gives us $S_T(\mathbf{x}, \mathbf{y}) = S_T(\mathbf{y}, \mathbf{x})$, which is a polynomial identity. Substituting a_U and b_U for X_U and Y_U in this identity implies $S_T(\mathbf{a}, \mathbf{b}) = S_T(\mathbf{b}, \mathbf{a})$. Since this holds for all T, $\mathbf{a} \oplus \mathbf{b} = \mathbf{b} \oplus \mathbf{a}$ in $\mathbf{W}_G(A)$ by the definition of $\oplus$.

Similar arguments using polynomial rings over $\mathbf{Z}$ first and then substitution homomorphisms from such rings to a general ring A lead to proofs of the remaining ring axioms for $\mathbf{W}_G(A)$. This is just like the classical case. For any ring homomorphism $f\colon A \to B$ define $\mathbf{W}_G(f)\colon \mathbf{W}_G(A) \to \mathbf{W}_G(B)$ by applying f to the coordinates:

$$\mathbf{W}_G(f)(\mathbf{a}) = (f(a_T))_{T\in\mathcal{F}(G)} \in \mathbf{W}_G(B).$$

Because the polynomials S_T and M_T have integral coefficients, $\mathbf{W}_G(f)$ is a ring homomorphism and composition of ring homomorphisms is respected, This is a ring homomorphism and makes $\mathbf{W}_G$ a covariant functor from commutative rings to commutative rings.

We previously saw that each Witt polynomial W_T defines a function $\mathbf{W}_G(A) \to A$ such that

$$W_T(\mathbf{a} \oplus \mathbf{b}) = W_T(\mathbf{a}) + W_T(\mathbf{b}) \text{ and } W_T(\mathbf{a} \odot \mathbf{b}) = W_T(\mathbf{a})W_T(\mathbf{b}).$$

Since $W_T(1, 0, 0, \dots) = 1$, $W_T\colon \mathbf{W}_G(A) \to A$ is a ring homomorphism. That Witt polynomials define ring homomorphisms out of $\mathbf{W}_G(A)$ will be very useful to us later. Packaging all the Witt polynomials together, we get a ring homomorphism $W : \mathbf{W}_G(A) \to \prod_{T\in\mathcal{F}(G)} A$ which is W_T in the T-th coordinate:

$$W(\mathbf{a}) = (W_T(\mathbf{a}))_{T\in\mathcal{F}(G)} = \left(\sum_{U\leq T} \varphi_T(U) a_U^{\#T/\#U}\right)_{T\in\mathcal{F}(G)}.$$

This homomorphism is called the *ghost map* and its coordinates $W_T(\mathbf{a})$ are called the *ghost components* of $\mathbf{a}$. In some cases it is quite useless: if G is pro-p and A has characteristic p then $W(\mathbf{a}) = (a_0^{\#T})_{T\in\mathcal{F}(G)}$, whose dependence on $\mathbf{a}$ only involves a_0. If A fits the hypothesis of Theorem 2.2 then the ghost map is injective (i.e., the ghost components of $\mathbf{a}$ determine $\mathbf{a}$). Also from Theorem 2.2 the ghost map is bijective if every integer $\varphi_T(T)$ is invertible in A so $\mathbf{W}_G(A) \cong \prod_{T\in\mathcal{F}(G)} A$ by the ghost map. That means $\mathbf{W}_G(A)$ is a new kind of ring only if some $\varphi_T(T)$ is not invertible in A, and especially if A has $\varphi_T(T)$-torsion for some T (e.g., G is a nontrivial pro-p group and A has characteristic p).

The coordinates on which a Witt vector is nonzero is called its *support*. While the ring operations in $\mathbf{W}_G(A)$ are generally not componentwise, addition in $\mathbf{W}_G(A)$ is componentwise on two Witt vectors with disjoint support.

Theorem 2.8. *Let $\{R, S\}$ be a partition of $\mathcal{F}(G)$, i.e., $R \cup S = \mathcal{F}(G)$ and $R \cap S = \emptyset$. For every ring A and any $\mathbf{a} \in \mathbf{W}_G(A)$, define $\mathbf{r}(\mathbf{a})$ and $\mathbf{s}(\mathbf{a})$ to be the Witt vectors derived from $\mathbf{a}$ with support in R and S:*

$$\mathbf{r}(\mathbf{a}) = \begin{cases} a_T & \textit{if } T \in R, \\ 0 & \textit{if } T \in S, \end{cases} \quad \textit{and} \quad \mathbf{s}(\mathbf{a}) = \begin{cases} 0 & \textit{if } T \in R, \\ a_T & \textit{if } T \in S. \end{cases}$$

Then $\mathbf{a} = \mathbf{r}(\mathbf{a}) + \mathbf{s}(\mathbf{a})$ in $\mathbf{W}_G(A)$.

The conclusion of Theorem 2.8 is well known in the classic $G = \mathbf{Z}_p$ case and the proof there is essential the same as the proof here. Specifically, one first demonstrates the identity using a generic coefficient ring of characteristic 0, say $\mathbf{Z}[\underline{X}]$. The result follows by functoriality as $\mathbf{Z}[\underline{X}]$ is a domain and the ghost map is an injection. We omit the proof due to space considerations, however the details are explained in full in [6].

Proof. First we will show the result in $\mathbf{W}_G(\mathbf{Z}[\underline{X}])$ for the particular Witt vector $\mathbf{x} = (X_T)_{T\in\mathcal{F}(G)}$: $\mathbf{x} = \mathbf{r}(\mathbf{x}) + \mathbf{s}(\mathbf{x})$ in $\mathbf{W}_G(\mathbf{Z}[\underline{X}])$. If we prove this then given any ring A and $\mathbf{a} \in \mathbf{W}_G(A)$, there is a ring homomorphism $f\colon \mathbf{Z}[\underline{X}] \to A$ such that $f(X_T) = a_T$ for all T, and applying the ring homomorphism $\mathbf{W}_G(f)\colon \mathbf{W}_G(\mathbf{Z}[\underline{X}]) \to \mathbf{W}_G(A)$ to the identity $\mathbf{x} = \mathbf{r}(\mathbf{x}) + \mathbf{s}(\mathbf{x})$ turns it into $\mathbf{a} = \mathbf{r}(\mathbf{a}) + \mathbf{s}(\mathbf{a})$.

Since $\mathbf{Z}[\underline{X}]$ is a domain of characteristic 0, the ghost map

$$W\colon \mathbf{W}_G(\mathbf{Z}[\underline{X}]) \to \prod_{T\in\mathcal{F}(G)} \mathbf{Z}[\underline{X}]$$

is an injective ring homomorphism, so it suffices to prove

$$W(\mathbf{x}) = W(\mathbf{r}(\mathbf{x}) + \mathbf{s}(\mathbf{x})).$$

The right side is $W(\mathbf{r}(\mathbf{x})) + W(\mathbf{s}(\mathbf{x}))$, which is a sum in the product ring $\prod_{T\in\mathcal{F}(G)} \mathbf{Z}[\underline{X}]$, so its T-th coordinate for any T is

$$W_T(\mathbf{r}(\mathbf{x})) + W_T(\mathbf{s}(\mathbf{x})) = \sum_{\substack{U\le T\\ U\in R}} \varphi_T(U) X_U^{\#T/\#U} + \sum_{\substack{U\le T\\ U\in S}} \varphi_T(U) X_U^{\#T/\#U}.$$

Since $R \cup S = \mathcal{F}(G)$ and $R \cap S = \emptyset$, each U with $U \le T$ will lie in exactly one of R or S, so

$$W_T(\mathbf{r}(\mathbf{x})) + W_T(\mathbf{s}(\mathbf{x})) = \sum_{U\le T} \varphi_T(U) X_U^{\#T/\#U} = W_T(\mathbf{x}).$$

Therefore $W(\mathbf{r}(\mathbf{x}) + \mathbf{s}(\mathbf{x}))$ and $W(\mathbf{x})$ have the same T-th component for all T, so they are equal, which shows $\mathbf{r}(\mathbf{x}) + \mathbf{s}(\mathbf{x}) = \mathbf{x}$. □

One typically proves an algebraic identity in $\mathbf{W}_G(A)$ by reformulating it as an identity in a ring of Witt vectors over a polynomial ring over $\mathbf{Z}$. From now on, we will usually prove the reformulation but may not go through the deduction of the identity we want over A from the identity proved over a polynomial ring; instead simply invoke functoriality.

From now on, when we prove an algebraic identity in $\mathbf{W}_G(A)$ by reformulating it as an identity in a ring of Witt vectors over a polynomial ring over $\mathbf{Z}$, we will usually prove the reformulation but may not go through the deduction of the identity we want over A from the identity proved over a polynomial ring, and instead simply invoke functoriality.

Definition 2.9. For $a \in A$ and $T \in \mathcal{F}(G)$, denote by $\omega_T(a) \in \mathbf{W}_G(A)$ the Witt vector with T-coordinate a and all other coordinates 0. We call $\omega_T(a)$ the T-th *Teichmüller lift* of a.

We denote the trivial G-set G/G as 0 and by $\omega_0(a)$ the G/G-th Teichmüller lift. The function $\omega_0 \colon A \to \mathbf{W}_G(A)$ generalizes the classical Teichmüller lift. Like the classical Teichmüller lift, ω_0 is multiplicative. For a general formula for $\omega_T(a)\omega_{T'}(b)$, see [4, p. 355].

An easy consequence of Theorem 2.8 is that any Witt vector $\mathbf{a}$ of finite support satisfies $\mathbf{a} = \sum_{U \in \mathrm{Supp}(\mathbf{a})} \omega_U(a_U)$ where Supp($\mathbf{a}$) is the support of $\mathbf{a}$. Theorem 2.20 will show the natural generalization $\mathbf{a} = \sum_{U \in \mathcal{F}(G)} \omega_U(a_U)$ makes sense in a suitable topology. We have the following multiplication formula for Teichmüller representatives.

Theorem 2.10. *For any $a \in A$ and $\mathbf{b} \in \mathbf{W}_G(A)$,*

$$\omega_0(a)\mathbf{b} = (a^{\#T} b_T)_{T \in \mathcal{F}(G)}.$$

In particular, $\omega_0(a)\omega_0(b) = \omega_0(ab)$.

Proof. By functoriality, it suffices to show in $\mathbf{W}_G(\mathbf{Z}[\underline{X}, \underline{Y}])$ that

$$(X_0, 0, 0, 0, \dots)(Y_T)_{T \in \mathcal{F}(G)} = (X_0^{\#T} Y_T)_{T \in \mathcal{F}(G)},$$

and to show this equation it suffices to prove the ghost components (Witt polynomial values) of both sides are equal. Since $W_T \colon \mathbf{W}_G(\mathbf{Z}[\underline{X}, \underline{Y}]) \to \mathbf{Z}[\underline{X}, \underline{Y}]$ is multiplicative,

$$\begin{aligned} W_T((X_0, 0, 0, 0, \dots)(Y_U)_{U \in \mathcal{F}(G)}) &= W_T(X_0, 0, 0, 0, \dots) W_T((Y_U)_{U \in \mathcal{F}(G)}) \\ &= X_0^{\#T} \sum_{U \le T} \varphi_T(U) Y_U^{\#T/\#U} \end{aligned}$$

and

$$W_T((X_0^{\#U} Y_U)_{U \in \mathcal{F}(G)}) = \sum_{U \le T} \varphi_T(U) (X_0^{\#U} Y_U)^{\#T/\#U} = \sum_{U \le T} \varphi_T(U) X_0^{\#T} Y_U^{\#T/\#U}.$$

□

The Witt polynomial $W_T(\underline{X})$ becomes homogeneous of degree $\#T$ if we give X_U degree $\#U$ (e.g., X_0 has degree 1, not 0). This grading makes the addition and multiplication polynomials homogeneous as well:

Theorem 2.11. *Give the ring $\mathbf{Z}[\underline{X}, \underline{Y}]$ the grading in which the degree of X_U and Y_U is $\#U$.*

(*a*) *For all T, the polynomial S_T is homogeneous of degree $\#T$ and M_T is homogeneous of degree $2\#T$.*

(*b*) *For all T, we have $S_T(\underline{X},\mathbf{0}) = X_T$, $S_T(\mathbf{0},\underline{Y}) = Y_T$, $M_T(\underline{X},\mathbf{0}) = 0$, and $M_T(\mathbf{0},\underline{Y}) = 0$.*

The second part of the theorem is saying S_T equals $X_T + Y_T$ plus monomials $X_U^i Y_V^j$ where $U < T$ and $V < T$ (we cannot have $U = T$ or $V = T$ by homogeneity), while M_T contains no monomials that are pure $\underline{X}$-terms or pure $\underline{Y}$-terms.

Proof. (a) We will work out the homogeneity for M_T; the argument for S_T is similar. Clearly $M_0(X_0, Y_0) = X_0 Y_0$, which is homogeneous of degree 2 and its only monomial term contains the factors X_0 and Y_0. Let $n \geq 2$ and assume by induction for all transitive G-sets U with $\#U < n$ that M_U is homogeneous of degree $2\#U$. Pick a transitive G-set T with $\#T = n$. (If there are no such G-sets then we are vacuously done.) Solving for M_T in (3) in $\mathbf{Q}[\underline{X},\underline{Y}]$,

$$\begin{aligned} M_T &= \frac{1}{\varphi_T(T)}\left(\sum_{U_1 \leq T} \varphi_T(U_1) X_{U_1}^{\frac{\#T}{\#U_1}} \sum_{U_2 \leq T} \varphi_T(U_2) Y_{U_2}^{\frac{\#T}{\#U_2}} - \sum_{U<T} \varphi_T(U) M_U^{\frac{\#T}{\#U}}\right) \\ &= \frac{1}{\varphi_T(T)}\left(\sum_{U_1,U_2 \leq T} \varphi_T(U_1)\varphi_T(U_2) X_{U_1}^{\frac{\#T}{\#U_1}} Y_{U_2}^{\frac{\#T}{\#U_2}} - \sum_{U<T} \varphi_T(U) M_U^{\frac{\#T}{\#U}}\right). \end{aligned}$$

By the inductive hypothesis, each M_U for $U < T$ is homogeneous of degree $2\#U$, so $M_U^{\#T/\#U}$ is homogeneous of degree $2\#T$. By the definition of the grading, $X_{U_1}^{\#T/\#U_1}$ has degree $\#T$ and $Y_{U_2}^{\#T/\#U_2}$ has degree $\#T$, so $X_{U_1}^{\#T/\#U_1} Y_{U_2}^{\#T/\#U_2}$ has degree $2\#T$.

(b) We will work out the result for multiplication polynomials. Since $M_0(\underline{X},\mathbf{0})$ is $X_0 0 = 0$, we may assume $T \neq 0$. Set every Y_U to 0 in the recursive formula for M_T above. Then the formula tells us $M_T(\underline{X},\mathbf{0})$ is equal to

$$\frac{1}{\varphi_T(T)}\left(\sum_{U_1,U_2 \leq T} \varphi_T(U_1)\varphi_T(U_2) X_{U_1}^{\#T/\#U_1} \cdot 0 - \sum_{U<T} \varphi_T(U) M_U(\underline{X},\mathbf{0})^{\#T/\#U}\right).$$

Using the inductive hypothesis, each term is 0. □

So the polynomials $S_T(\{X_U^{\#U}, Y_U^{\#U}\}_{U \in \mathcal{F}(G)})$ are genuine homogeneous polynomials of degree $\#T$ (replace X_U and Y_U with their $\#U$-th powers everywhere), and similarly for the multiplication polynomials.

Corollary 2.12. *For $n \in \mathbf{Z}^+$, suppose $\mathbf{a}, \mathbf{b} \in \mathbf{W}_G(A)$ satisfy $a_U = 0$ and $b_U = 0$ when $\#U < n$. Then for any T with $\#T = n$, $(\mathbf{a}+\mathbf{b})_T = a_T + b_T$.*

Proof. By definition, $(\mathbf{a}+\mathbf{b})_T = S_T(\mathbf{a},\mathbf{b})$, and on the right side $\mathbf{a}$ and $\mathbf{b}$ only matter in their coordinates at $U \leq T$. By Theorem 2.11, $S_T(\underline{X},\underline{Y})$ equals $X_T + Y_T$ plus other monomials which each involve only X_U's for $U < T$ and Y_V's for $V < T$. Setting X_U and Y_U equal to a_U and b_U for $U \leq T$ respectively, we obtain $S_T(\mathbf{a},\mathbf{b}) = a_T + b_T$. □

2.1 Projections and topology

We can consider any G/N-set T as a G-set by defining the action of $g \in G$ on an element $x \in T$ to be $g \cdot x := gN \cdot x$. A G-set arises in this way from a G/N-set precisely when N acts trivially on it. A G/N-set is transitive as a G/N-set if and only if it's transitive as a G-set since its G/N-orbits and G-orbits are the same. Writing a transitive G-set as G/H, N acts trivially on it if and only if $N \subset H$, in which case we can write G/H as $(G/N)/(H/N)$ to see it as a G/N-set. Two G/N-sets are isomorphic if and only if they are isomorphic when viewed as G-sets. So turning G/N-sets into G-sets gives us an embedding of $\mathcal{F}(G/N)$ into $\mathcal{F}(G)$ and the image of $\mathcal{F}(G/N)$ in $\mathcal{F}(G)$ is all $T \in \mathcal{F}(G)$ on which N acts trivially. For $T \in \mathcal{F}(G)$ which is in the image of $\mathcal{F}(G/N)$, write $T \cong G/H$ as a G-set with $N \subset H$. If $T' \leq T$ then we can write $T' \cong G/H'$ where $H \subset H'$, so $N \subset H'$. Therefore the embedding of $\mathcal{F}(G/N)$ into $\mathcal{F}(G)$ is "full" as a partially ordered subset in the sense that all finite transitive G-sets below a G-set in the image are also in the image. For any *closed* normal subgroup N of G the quotient G/N is a profinite group and there is a natural group homomorphism from G onto G/N. Identifying $\mathcal{F}(G/N)$ with its image in $\mathcal{F}(G)$, there is a natural projection map

$$\begin{array}{rcl} \mathrm{Proj}^G_{G/N} : \mathbf{W}_G(A) & \to & \mathbf{W}_{G/N}(A) \\ \mathbf{a} & \mapsto & (a_T)_{T \in \mathcal{F}(G/N)}. \end{array}$$

This is trivially surjective and is a ring homomorphism.

Example 2.13. The ring homomorphism $\mathbf{W}_{\mathbf{Z}_p}(A) \to \mathbf{W}_{\mathbf{Z}_p/p^n\mathbf{Z}_p}(A)$ is the classical truncation homomorphism from $\mathbf{W}(A)$ onto the length $n+1$ Witt vectors $\mathbf{W}_{n+1}(A)$.

If G and H are profinite groups and there is a continuous surjective group homomorphism $G \twoheadrightarrow H$ then there is a surjective ring homomorphism $\mathbf{W}_G(A) \twoheadrightarrow \mathbf{W}_H(A)$ since we can realize H as some G/N and the map $G \twoheadrightarrow H$ as reduction mod N.

Example 2.14. For any $d \geq 2$ and field k of characteristic p, $\mathbf{W}_{\mathbf{Z}_p}(k)$ is a homomorphic image of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ since $\mathbf{Z}_p$ is a continuous homomorphic image of $\mathbf{Z}_p^d$ (in many ways). Since $\mathbf{W}_{\mathbf{Z}_p}(k)$ is a domain, we obtain as kernels many non-maximal prime ideals of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$. We will see in Section 6 that this does not give us all the non-maximal prime ideals when $d = 2$.

Example 2.15. For any $d \geq 2$, the ring $\mathbf{W}_{\mathbf{Z}_p^d}(A)$ has $\mathbf{W}_{\mathbf{Z}_p^2}(A)$ as a homomorphic image, since the group $\mathbf{Z}_p^d$ has $\mathbf{Z}_p^2$ as a continuous homomorphic image.

Definition 2.16. For any closed normal subgroup $N \lhd G$, set

$$\begin{array}{rcl} K_N = \ker(\mathrm{Proj}^G_{G/N}) & = & \{\mathbf{a} \in \mathbf{W}_G(A) : a_T = 0 \text{ for all } T \in \mathcal{F}(G/N)\} \\ & = & \{\mathbf{a} \in \mathbf{W}_G(A) : a_T = 0 \text{ when } N \text{ acts trivially on } T\}. \end{array}$$

The kernel K_N is an ideal of $\mathbf{W}_G(A)$ and the rings $\mathbf{W}_G(A)/K_N$ and $\mathbf{W}_{G/N}(A)$ are isomorphic.

Example 2.17. Taking $N = G$, $K_G = \{\mathbf{a} \in \mathbf{W}_G(A) : a_0 = 0\}$ and the quotient $\mathbf{W}_G(A)/K_G \cong W_0(A) = A$. If A is a domain (field) then K_G is a prime (maximal) ideal in $\mathbf{W}_G(A)$.

(To be more explicit in its dependence on the group and the ring, we could write K_N as $K_N(G, A)$, but we will leave this dependence out of the notation unless it is important to be explicit about it.) If $N \subset N'$ and $a_T = 0$ whenever N acts trivially on T then $a_T = 0$ whenever N' acts trivially on T, so $K_N \subset K_{N'}$. For open normal subgroups N and N', the groups G/N and G/N' are finite. The rings $\mathbf{W}_{G/N}(A)$ for open normal N with the ring homomorphisms

$$\mathrm{Proj}^{G/N}_{G/N'} : \mathbf{W}_{G/N}(A) \to \mathbf{W}_{G/N'}(A)$$

when $N \subset N'$ form a projective system and it is isomorphic to the projective system of rings $\mathbf{W}_G(A)/K_N$ and natural ring homomorphisms $\mathbf{W}_G(A)/K_N \to \mathbf{W}_G(A)/K_{N'}$ when $N \subset N'$.

We have $\mathbf{W}_G(A) \cong \varprojlim_N \mathbf{W}_{G/N}(A) \cong \varprojlim_N \mathbf{W}_G(A)/K_N$ as rings, where the inverse limits are taken over open normal subgroups of G ordered by reverse inclusion. This gives $\mathbf{W}_G(A)$ a topology as a closed subset of the product $\prod_N \mathbf{W}_{G/N}(A) \cong \prod_N \mathbf{W}_G(A)/K_N$, where N runs over the open normal subgroups of G and each factor $\mathbf{W}_{G/N}(A)$ and $\mathbf{W}_G(A)/K_N$ is given the discrete topology. This topology on $\mathbf{W}_G(A)$ is called the *profinite topology.*

The profinite topology on $\mathbf{W}_G(A)$ is Hausdorff since any subspace of a product of discrete spaces is Hausdorff. The ring $\mathbf{W}_G(A)$ is compact in its profinite topology if and only if A is finite.

To say $\mathbf{a}$ and $\mathbf{b}$ are near each other in the profinite topology means $\mathbf{a} \equiv \mathbf{b} \bmod K_N$ for some "small" open normal subgroup N in G; the larger $[G : N]$ is, the closer $\mathbf{a}$ and $\mathbf{b}$ are. How can we tell in terms of coordinates of $\mathbf{a}$ and $\mathbf{b}$ that $\mathbf{a} \equiv \mathbf{b} \bmod K_N$? While K_N is described by Definition 2.16 for all closed N, when N is open the set G/N belongs to $\mathcal{F}(G)$ and $\mathcal{F}(G/N)$ is a "full" subset of $\mathcal{F}(G)$, so we can describe K_N a little differently than in Definition 2.16:

$$K_N = \{\mathbf{a} \in \mathbf{W}_G(A) : a_T = 0 \text{ for all } T \in \mathcal{F}(G) \text{ such that } T \leq G/N\}. \tag{6}$$

Lemma 2.18. *For any open normal subgroup N of G,*

$$\mathbf{a} \equiv \mathbf{b} \bmod K_N \iff a_T = b_T \textit{ for all } T \leq G/N.$$

Proof. Assume $a_T = b_T$ for $T \leq G/N$. Using Theorem 2.8 with the partition of $\mathcal{F}(G)$ being $\{T \leq G/N\} \cup (\mathcal{F}(G) - \{T \leq G/N\})$, we can write $\mathbf{a} = \mathbf{a}_1 + \mathbf{a}_2$ where $\mathbf{a}_1$ is supported on $T \leq G/N$ and $\mathbf{a}_2$ is supported on the complement, so $\mathbf{a}_2 \in K_N$. Similarly write $\mathbf{b} = \mathbf{b}_1 + \mathbf{b}_2$. Then $\mathbf{a}_1 = \mathbf{b}_1$, so $\mathbf{a} - \mathbf{b} = \mathbf{a}_2 - \mathbf{b}_2 \in K_N$.

Conversely, assume $\mathbf{a} \equiv \mathbf{b} \bmod K_N$ and write $\mathbf{a} = \mathbf{b} + \mathbf{c}$ for $\mathbf{c} \in K_N$. Since $S_0(\underline{X}, \underline{Y}) = X_0 + Y_0$, we have $a_0 = b_0 + c_0$. Since $c_0 = 0$, $a_0 = b_0$. If G/N is trivial we are done. Otherwise, let T be a nontrivial G-set with $T \leq G/N$. Since the polynomial $S_T(\underline{X}, \underline{Y})$ only depends on Y_U for $U \leq T$, and $c_U = 0$ for all $U \leq T$, evaluating S_T with $Y_U = c_U$ for all U or $Y_U = 0$ for all U leads to the same result. Therefore $a_T = S_T(\mathbf{b}, \mathbf{c}) = S_T(\mathbf{b}, \mathbf{0}) = b_T$, where the last equality follows from Theorem 2.11(b). □

Theorem 2.19. *The ring $\mathbf{W}_G(A)$ is complete in the profinite topology.*

Proof. It suffices to show any Cauchy net converges. Let $\{\mathbf{a}_i\}_{i \in I}$ be a Cauchy net in $\mathbf{W}_G(A)$ for the profinite topology.

For each open normal subgroup $N \lhd G$ there is an $i_N \in I$ such that for all $i, j \geq i_N$, $\mathbf{a}_i \equiv \mathbf{a}_j \bmod K_N(G, A)$, which by Lemma 2.18 means $(\mathbf{a}_i)_T = (\mathbf{a}_j)_T$ for all $T \leq G/N$.

For each T, pick N so that $T \leq G/N$ and let a_T be the common value of $(\mathbf{a}_i)_T$ for all $i \geq i_N$. This is independent of the choice of N. Let $\mathbf{a}$ be the Witt vector with T-th coordinate a_T for all T. We will show this is the limit of the $\mathbf{a}_i$'s.

For an open normal subgroup N of G and $i \geq i_N$, $a_T = (\mathbf{a}_i)_T$ for all $T \leq G/N$. So by Lemma 2.18 $\mathbf{a} \equiv \mathbf{a}_i \bmod K_N(G, A)$ for $i \geq i_N$. Thus $\lim \mathbf{a}_i = \mathbf{a}$ in the profinite topology. □

Theorem 2.8, which trivially extends from a two-element partition of $\mathcal{F}(G)$ to any finite partition, extends with the profinite topology on $\mathbf{W}_G(A)$ to suitable infinite partitions of $\mathcal{F}(G)$.

Theorem 2.20. *Let $\mathcal{F}(G) = \bigcup_{i \in I} R_i$ be a partition where the index set I is a directed set such that for all $j \in I$, the set $\{i \in I : i \leq j\}$ is finite. For any $\mathbf{a} \in \mathbf{W}_G(A)$, let $\mathbf{r}_i(\mathbf{a})$ be the Witt vector in $\mathbf{W}_G(A)$ which is the part of $\mathbf{a}$ supported on R_i:*

$$\mathbf{r}_i(\mathbf{a}) = \begin{cases} a_T, & \text{if } T \in R_i, \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$\mathbf{a} = \lim_{j \in I} \sum_{i \leq j} \mathbf{r}_i(\mathbf{a}),$$

where the limit is taken in the profinite topology on $\mathbf{W}_G(A)$. In particular,

$$\mathbf{a} = \lim_{T \in \mathcal{F}(G)} \sum_{U \leq T} \omega_U(a_U).$$

Proof. Consider the net $\{\mathbf{s}_j\}_{j \in I}$ in $\mathbf{W}_G(A)$ defined by $\mathbf{s}_j = \sum_{i \leq j} \mathbf{r}_i(\mathbf{a})$. Notice for each j the sum $\sum_{i \leq j} \mathbf{r}_i(\mathbf{a})$ has finitely many terms by hypothesis. We aim to show $\{\mathbf{s}_j\}_{j \in I}$ converges to $\mathbf{a}$ in the profinite topology, that is to say for each open normal subgroup N of G there is $j_N \in I$ such that for all $j \geq j_N$, $\mathbf{s}_j \equiv \mathbf{a} \bmod K_N$. By Lemma 2.18 this means the T-th components of $\mathbf{s}_j$ and $\mathbf{a}$ agree for all $j \geq j_N$ and $T \leq G/N$.

For each $T \leq G/N$, there is a unique index $i_T \in I$ such that $T \in R_{i_T}$. Therefore $\mathbf{r}_{i_T}(\mathbf{a})_T = a_T$. Let $S_N = \{i_T : T \leq G/N\}$. This is a finite set of indices in I. If $i \notin S_N$ then $T \notin R_i$ for all $T \leq G/N$, so $\mathbf{r}_i(\mathbf{a})_T = 0$ when $T \leq G/N$. Letting $R = I \setminus S_N$, $\mathbf{a} = \sum_{i \in S_N} \mathbf{r}_i(\mathbf{a}) + \mathbf{r}_R(\mathbf{a})$ by an extension of Theorem 2.8 to finite partitions of $\mathcal{F}(G)$. If $T \leq G/N$ then $i_T \notin R$, so $\mathbf{r}_R(\mathbf{a})_T = 0$. Therefore $\mathbf{r}_R(\mathbf{a}) \equiv 0 \bmod K_N$ so

$$\mathbf{a} \equiv \sum_{i \in S_N} \mathbf{r}_i(\mathbf{a}) \bmod K_N. \tag{7}$$

Since I is directed and S_N is finite, there is an index $j_N \in I$ such that $j_N \geq i$ for all $i \in S_N$. For all $j \geq j_N$, $S_N \subset \{i \in I : i \leq j\}$, so

$$\mathbf{s}_j = \sum_{i \leq j} \mathbf{r}_i(\mathbf{a}) = \sum_{i \in S_N} \mathbf{r}_i(\mathbf{a}) + \sum_{\substack{i \leq j \\ i \notin S_N}} \mathbf{r}_i(\mathbf{a}).$$

Reducing mod K_N, the first summand is congruent to $\mathbf{a}$ mod K_N by (7) whereas the second summand is congruent to $0 \bmod K_N$. The last conclusion is clear using the partition of $\mathcal{F}(G)$ into singleton subsets. □

Example 2.21. If G is a pro-p group and k is a perfect field (or just a perfect ring) of characteristic p then we can write any $a_U \in k$ in the form $b_U^{\#U}$ for some $b_U \in k$, so

$$\mathbf{a} = \lim_{T \in \mathcal{F}(G)} \sum_{U \leq T} \omega_U(b_U^{\#U}) = \lim_{T \in \mathcal{F}(G)} \sum_{U \leq T} \omega_0(b_U)\omega_U(1)$$

by Theorem 2.10. This last series is the usual p-adic expansion of a Witt vector when $G = \mathbf{Z}_p$: $\omega_U(1) = p^n$ when $U = \mathbf{Z}_p/p^n\mathbf{Z}_p$ and $\lim_{T \in \mathcal{F}(\mathbf{Z}_p)} = \lim_{n \to \infty}$.

3 Comparing Topologies

In the profinite topology on $\mathbf{W}_G(A)$, an element $\mathbf{a}$ is small if $a_T = 0$ for all T on which a small open normal subgroup of G (one of large index in G) acts trivially. There is another notion of being small: $\mathbf{a}$ is small when $a_T = 0$ for all T of size below a given bound. This topology is defined by another family of ideals.

Definition 3.1. For $n \in \mathbf{Z}^+$, set

$$I_n(G, A) = \{\mathbf{a} \in \mathbf{W}_G(A) : a_T = 0 \text{ for } \#T < n\}.$$

These are the Witt vectors $\mathbf{a}$ with support in $\{T : \#T \geq n\}$.

Lemma 3.2. *Each $I_n(G, A)$ is an ideal in $\mathbf{W}_G(A)$.*

Proof. Each addition polynomial S_T depends only on variables indexed by (isomorphism classes of) finite transitive G-sets $U \leq T$ and has no constant term by Theorem 2.11. So if two Witt vectors are in $I_n(G,A)$ then their sum is also in $I_n(G,A)$.

It remains to show for any $\mathbf{a} \in \mathbf{W}_G(A)$ and $\mathbf{b} \in I_n(G,A)$ that $\mathbf{ab} \in I_n(G,A)$. Set $\mathbf{c} = \mathbf{ab}$. By the definition of multiplication in $\mathbf{W}_G(A)$, $c_T = M_T(\mathbf{a},\mathbf{b})$ for any T. If $\#T < n$, $b_U = 0$ for $U \leq T$ by hypothesis. Since $M_T(\underline{X},\underline{Y})$ only depends on Y_U for $U \leq T$, $c_T = M_T(\mathbf{a},\mathbf{b}) = M_T(\mathbf{a},\mathbf{0})$ and $M_T(\mathbf{a},\mathbf{0}) = 0$ by Theorem 2.11. □

Obviously the ideals $I_n(G,A)$ are decreasing:

$$\mathbf{W}_G(A) = I_1(G,A) \supset I_2(G,A) \supset \cdots \supset I_n(G,A) \supset I_{n+1}(G,A) \supset \cdots .$$

Since $\bigcap_{n\geq 1} I_n(G,A) = \{\mathbf{0}\}$, we can put a Hausdorff topology on $\mathbf{W}_G(A)$ so that the collection of ideals $\{I_n(G,A)\}_{n\geq 1}$ form a fundamental system of neighborhoods of $\mathbf{0}$: a nonempty subset $\mathcal{O} \subset \mathbf{W}_G(A)$ is open in this topology if for each $\mathbf{a} \in \mathcal{O}$ the coset $\mathbf{a} + I_n(G,A)$ is in $\mathcal{O}$ for some n. This is called the *initial vanishing topology.*

Remark 3.3. Of course it could happen that $I_n(G,A) = I_{n+1}(G,A)$, namely if there are no open subgroups of G with index n. If G is an infinite pro-p group, then the different ideals in this filtration are indexed by p-powers, and ideals indexed by different powers of p are different from each other since there are open subgroups of each p-power index in G:

$$I_{p^m}(G,A) = \{\mathbf{a} : a_T = 0 \text{ for } \#T < p^m\} = \{\mathbf{a} : a_T = 0 \text{ for } \#T \leq p^{m-1}\}$$

and

$$\mathbf{W}_G(A) = I_1(G,A) \supsetneqq I_p(G,A) \supsetneqq \cdots \supsetneqq I_{p^m}(G,A) \supsetneqq I_{p^{m+1}}(G,A) \supsetneqq \cdots .$$

The next lemma is an analogue of Lemma 2.18.

Lemma 3.4. *For $n \geq 1$ and $\mathbf{a}$ and $\mathbf{b}$ in $\mathbf{W}_G(A)$, $\mathbf{a} \equiv \mathbf{b} \bmod I_n(G,A)$ if and only if $a_T = b_T$ for all $T \in \mathcal{F}(G)$ such that $\#T < n$.*

Proof. An argument similar to the proof of Lemma 2.18 can be used. □

Theorem 3.5. *The ring $\mathbf{W}_G(A)$ is complete in the initial vanishing topology.*

Proof. Since the topology is defined by a countable set of ideals, it suffices to show any Cauchy sequence (rather than Cauchy net) converges. Let $\{\mathbf{a}_i\}_{i\in\mathbf{N}}$ be a Cauchy sequence in $\mathbf{W}_G(A)$ for the initial vanishing topology. We will construct a candidate limit and then show it works.

For each $n \geq 1$ there is an integer $N_n \in \mathbf{Z}^+$ such that for all $r, s \geq N_n$, $\mathbf{a}_r \equiv \mathbf{a}_s \bmod I_n(G,A)$, which by Lemma 3.4 means $(\mathbf{a}_r)_T = (\mathbf{a}_s)_T$ for all $T \in \mathcal{F}(G)$ such that $\#T < n$. We may choose the numbers N_n so that $N_1 < N_2 < N_3 < \cdots$.

For each T, pick $n > \#T$ and let a_T be the common value of $(\mathbf{a}_r)_T$ for all $r \geq N_n$. This is independent of the choice of n. Let $\mathbf{a}$ be the Witt vector with T-th coordinate a_T for all T. We will show this is the limit of the $\mathbf{a}_r$'s.

For each $n \geq 1$ and $T \in \mathcal{F}(G)$ with $\#T < n$, $a_T = (\mathbf{a}_r)_T$ for $r \geq N_n$, so by Lemma 3.4 $\mathbf{a} \equiv \mathbf{a}_r \bmod I_n(G, A)$ for $r \geq N_n$. Thus $\lim_{r\to\infty} \mathbf{a}_r = \mathbf{a}$ in the initial vanishing topology. □

Set $I_n = I_n(G, A)$. How do the profinite and initial vanishing topologies, defined by the families of ideals $\{K_N\}_{N \text{ open}}$ and $\{I_n\}_{n\geq 1}$, compare with each other?

Lemma 3.6. *Given finitely many finite transitive G-sets $T_1, \ldots, T_m$, there is an open normal subgroup N in G such that $G/N \geq T_i$ for $1 \leq i \leq m$.*

Proof. The frame $\mathcal{F}(G)$ is a directed set, so there is a $T \in \mathcal{F}(G)$ with $T \geq T_i$ for $i = 1, \ldots, m$. Since the G-sets with normal stabilizers are cofinal in $\mathcal{F}(G)$, we can take $T = G/N$ with N normal. □

Theorem 3.7. *Every K_N, for open normal N, is open in the initial vanishing topology on $\mathbf{W}_G(A)$. If G is topologically finitely generated then the profinite topology and the initial vanishing topology on $\mathbf{W}_G(A)$ are the same.*

Proof. Let N be an open normal subgroup of G. Since K_N is an additive group, to show it is open in the initial vanishing topology it suffices (and in fact is equivalent) to show there is an $n \geq 1$ such that $I_n \subset K_N$. Let n be any integer exceeding $[G : N]$. Then $T \leq G/N \Rightarrow \#T < n$, so for all $\mathbf{a} \in \mathbf{W}_G(A)$ we have

$$a_T = 0 \text{ for } \#T < n \Longrightarrow a_T = 0 \text{ for } T \leq G/N.$$

Thus $I_n \subset K_N$.

Now assume G is topologically finitely generated. Since I_n is an additive group, to show I_n is open in the profinite topology on $\mathbf{W}_G(A)$ it suffices to find an open normal subgroup $N \lhd G$ such that $K_N \subset I_n$. The key fact we use about a topologically finitely generated profinite group is that it has finitely many open subgroups of each index [12, p. 45], and thus $\{T : \#T < n\}$ is finite for all n. Therefore Lemma 3.6 tells us there is an open normal subgroup $N \lhd G$ such that $\#T < n \Rightarrow T \leq G/N$, so $K_N \subset I_n$. □

When G is topologically finitely generated, so $\{T : \#T = n\}$ is finite for every n, Theorem 2.20 implies

$$\mathbf{a} = \sum_{n\geq 1} \sum_{\#T=n} \omega_T(a_T)$$

for all $\mathbf{a}$ in $\mathbf{W}_G(A)$, where we use the partition $\mathcal{F}(G) = \bigcup_{n\geq 1} R_n$ for $R_n = \{T : \#T = n\}$.

Remark 3.8. For open normal subgroup N in G, to say $K_N \subset I_n$ is the same as saying $\#T < n \Rightarrow T \leq G/N$. Since $[G : N] < \infty$, there are only finitely many open subgroups of G containing

N, so if $K_N \subset I_n$ for some N there can be only finitely many T in $\mathcal{F}(G)$ with size less than n. Considering this over all n, the profinite topology and the initial vanishing topology on $\mathbf{W}_G(A)$ are equal if and only if G has finitely many conjugacy classes of open subgroups of each index.

The last general item we want to check with the ideals I_n is how they behave under multiplication. Is $I_m I_n \subset I_{mn}$? For pro-p groups satisfying a mild technical condition (which is always true when the group is abelian) we will see that the containment $I_{p^m} I_{p^n} \subset I_{p^{m+n}}$ holds in cases that are likely to be of most interest and in other cases it need not hold.

Before we can state the main result on products of these ideals for G a pro-p group and A a ring of characteristic p, we first make use of some properties of $\varphi_T(U)$. When G is a nontrivial pro-p group and H is a proper open subgroup, $\mathrm{Aut}_G(G/H) \cong \mathrm{N}_G(H)/H$ is a nontrivial p-group since $H \neq \mathrm{N}_G(H)$. Therefore $\varphi_T(T) \equiv 0 \bmod p$ when T is nontrivial.

Lemma 3.9. *If G is a pro-p group and $T \geq U$ in $\mathcal{F}(G)$ with U nontrivial, then $\varphi_T(U) \equiv 0 \bmod p$.*

Proof. Since U is nontrivial, G is not the trivial group. Consider the action of $\mathrm{Aut}_G(U)$ on the finite set of G-maps $T \to U$ where the action of $\alpha \in \mathrm{Aut}_G(U)$ on a G-map $f\colon T \to U$ is given by composition. Since $\mathrm{Aut}_G(U)$ is a p-group, the basic fixed-point congruence for actions by finite p-groups tells us that

$$\varphi_T(U) = \#\mathrm{Map}_G(T,U) \equiv \#\mathrm{Fix}(\mathrm{Map}_G(T,U)) \bmod p,$$

where we are counting fixed points of $\mathrm{Aut}_G(U)$ on the right. If a G-map $f\colon T \to U$ is fixed by $\mathrm{Aut}_G(U)$ then $\alpha(f(t)) = f(t)$ for all $\alpha \in \mathrm{Aut}_G(U)$ and $t \in T$. Since any G-map $T \to U$ is surjective, we get $\alpha(u) = u$ for all $u \in U$. Hence $\mathrm{Aut}_G(U)$ is trivial, which means U is trivial, which is a contradiction. Thus the set of fixed points is empty, so $\varphi_T(U) \equiv 0 \bmod p$. □

If U is trivial then $\varphi_T(U) = 1$, so we need U nontrivial in Lemma 3.9.

Example 3.10. If G is a pro-p group then $0 < U \leq T \Rightarrow \varphi_T(U)$ is a multiple of p by Lemma 3.9, so $W_T(\underline{X}) \equiv X_0^{\#T} \bmod p\mathbf{Z}[\underline{X}]$ for all $T \in \mathcal{F}(G)$. Therefore if A is a ring of characteristic p then $W_T(\mathbf{a}) = a_0^{\#T}$ for all T, and this depends on no a_U except a_0, so we definitely can't write a random element of $\prod_{T\in\mathcal{F}(G)} A$ in the form $(W_T(\mathbf{a}))_{T\in\mathcal{F}(G)} = (a_0^{\#T})_{T\in\mathcal{F}(G)}$, unless G is trivial and A is a perfect ring. Compare this with Example 2.4.

To motivate the divisibility conditions we will need on the numbers $\varphi_T(U)$ when G is a pro-p group, we state two lemmas about divisibility of $\varphi_T(U)$ for an arbitrary profinite group G which are general facts about group actions.

Lemma 3.11. *Let T and U be finite transitive G-sets with $U \leq T$. Then $\#U$ is a factor of $\#T$ and the fibers of any G-map $f : T \to U$ have size $\#T/\#U$.*

Proof. Pick $x_0 \in T$ and let $H = \mathrm{Stab}_{x_0}$ and $K = \mathrm{Stab}_{f(x_0)}$. Then $H \subset K$ and there are G-set isomorphisms $T \cong G/H$ and $U \cong G/K$ such that the following diagram commutes.

$$\begin{tikzcd}
T \arrow[r, "f"] \arrow[d, "gx_0 \mapsto gH"'] & U \arrow[d, "gf(x_0) \mapsto gK"] \\
G/H \arrow[r, "gH \mapsto gK"'] & G/K
\end{tikzcd} \tag{8}$$

So we may assume $T = G/H$, $U = G/K$, and $f(gH) = gK$ for all $g \in G$. Since $[G : H] = [G : K][K : H]$, $\#T = \#U[K : H]$. Therefore $\#T/\#U = [K : H]$ is a positive integer.

The fiber of f over a coset $g'K$ is $\{gH : gK = g'K\}$. How many different cosets gH have $gK = g'K$? We must have $g = g'k$ for some $k \in K$, so $gH = g'kH$, and the converse holds as well: for any $k \in K$, $f(g'kH) = g'kK = g'K$. So the fiber over $g'K$ is $\{g'kH : k \in K\}$. We need to determine when $g'k_1H = g'k_2H$ for k_1 and k_2 in K. This happens precisely when $k_1H = k_2H$, so the size of a fiber of f is the number of left H-cosets in K, which is $[K : H] = \#T/\#U$. □

Lemma 3.12. *For any profinite group G, let $T, U \in \mathcal{F}(G)$. Then $\varphi_T(T)$ divides $\varphi_T(U)\#T/\#U$.*

This generalizes the relation $\varphi_T(T)|\#T$ (i.e., $[\mathrm{N}_G(H) : H]|[G : H]$), which is the special case that U is trivial. If the stabilizer of T is normal then $\varphi_T(U) = \#U$ for all $U \leq T$, so the divisibility relations in Lemma 3.12 need not be strict when $U < T$.

Proof. If $\varphi_T(U) = 0$ then there is nothing to show. So we may assume $\varphi_T(U) > 0$, i.e., there are G-maps $T \to U$. Fixing $u_0 \in U$, the group $\mathrm{Aut}_G(T)$ acts on the set

$$X = \{(f, t) : f \in \mathrm{Map}_G(T, U), t \in T, f(t) = u_0\}$$

by $\psi(f, t) = (f\psi^{-1}, \psi(t))$. If $\psi(f, t) = (f, t)$ then $\psi(t) = t$ and $\psi(gt) = g\psi(t) = gt$ for all $g \in G$, so ψ is the identity on T and the action is free. Therefore every $\mathrm{Aut}_G(T)$-orbit in X has size $\#\mathrm{Aut}_G(T) = \varphi_T(T)$, which means $\#X$ is divisible by $\varphi_T(T)$. By Lemma 3.11, $\#X = \varphi_T(U)(\#T/\#U)$, so we are done. □

Now returning to the pro-p setting, we have the following divisibility condition on $\varphi_T(U)$.

Lemma 3.13. *Let G be a nontrivial pro-p group, $U < T$ in $\mathcal{F}(G)$ and $s \in p\mathbf{Z}$. Then*

$$\frac{\varphi_T(U)}{\varphi_T(T)} s^{\#T/\#U} \equiv 0 \bmod p\mathbf{Z}.$$

Proof. Write $\#T/\#U = p^r$ with $r \geq 1$. Setting $s = pm$,

$$\frac{\#U}{\#T} s^{\#T/\#U} = p^{-r} p^{p^r} m^{p^r} = p^{p^r - r} m^{p^r}.$$

Since $p \geq 2$ and $r \geq 1$, $p^r - r \in \mathbf{Z}^+$. Therefore $(\#U/\#T)s^{\#T/\#U}$ is an integeral multiple of p.

By Lemma 3.12, $\varphi_T(T)|\varphi_T(U)(\#T/\#U)$, so $(\varphi_T(U)\#T)/(\varphi_T(T)\#U)$ is an integer. Thus

$$\frac{\varphi_T(U)}{\varphi_T(T)} s^{\#T/\#U} = \left(\frac{\varphi_T(U)\#T}{\varphi_T(T)\#U}\right) \frac{\#U}{\#T} s^{\#T/\#U} \equiv 0 \bmod p\mathbf{Z}.$$

□

Definition 3.14. A pro-p group G is said to have the *ratio property* when the following holds: for all finite transitive G-sets T, T_1, and T_2 such that $T \geq T_1$, $T \geq T_2$, and $\#T < \#T_1\#T_2$, the ratio $\varphi_T(T_1)\varphi_T(T_2)/\varphi_T(T)$ is an integral multiple of p.

If T is a normal G-set, $\varphi_T(U) = \#U$ for any $U \leq T$, so the ratio $\varphi_T(T_1)\varphi_T(T_2)/\varphi_T(T)$ is $\#T_1\#T_2/\#T$, which is a power of p greater than 1. Therefore the ratio property is true when G is a pro-p abelian group. Even though this property was only defined for pro-p groups, one can define this in more generality (see discussion) and in this context it has been computationally verified using GAP for all dihedral groups of order a power of 2 up to 1200.

The ratio property was found because of its role in the proof of Theorem 3.16 below. Passing from G to G/N where N acts trivially on T, the ratio property for T, T_1 and T_2 can be viewed in $\mathcal{F}(G/N)$, so Definition 3.14 can be checked for all finite quotients of G to show it is true for G. Therefore, the ratio property is really a hypothesis about finite p-groups.

Lemma 3.15. *Let G be a pro-p group that satisfies the ratio property and A be a ring of characteristic p. Let $V \in \mathcal{F}(G)$ with $\#V \leq p^{m+n}$ for positive integers m and n. Consider Witt vectors* $\mathbf{a}$ *and* $\mathbf{b}$ *in $\mathbf{W}_G(A)$ such that $a_U = 0$ for all $U < V$ such that $\#U < p^m$ and $b_U = 0$ for all $U < V$ such that $\#U < p^n$. Set $\mathbf{c} = \mathbf{ab}$. Then $c_V = 0$.*

Proof. This will follow from functoriality by proving the following mod p congruence for particular Witt vectors over the ring $R = \mathbf{Z}[\underline{X}, \underline{Y}]$. Define $\mathbf{x}, \mathbf{y} \in \mathbf{W}_G(R)$ by

$$x_T = \begin{cases} 0, & \#T < p^m \text{ and } T < V, \\ X_T, & \text{otherwise,} \end{cases} \quad \text{and } y_T = \begin{cases} 0, & \#T < p^n \text{ and } T < V, \\ Y_T, & \text{otherwise.} \end{cases}$$

Set $\mathbf{z} = \mathbf{xy}$. We will show that

$$T \leq V \Longrightarrow z_T \equiv 0 \bmod pR. \tag{9}$$

Let's see how this implies the theorem. There is a ring homomorphism $f : R \to A$ such that $f(X_T) = a_T$ and $f(Y_T) = b_T$ for all $T \in \mathcal{F}(G)$. Then $\mathbf{W}_G(f)(\mathbf{x}) = \mathbf{a}$ and $\mathbf{W}_G(f)(\mathbf{y}) = \mathbf{b}$. The product $\mathbf{ab} = \mathbf{W}_G(f)(\mathbf{z})$ has T-component $f(z_T)$ and by (9) this lies in $f(pR) \subset pA = 0$ when $T \leq V$. Returning to the proof of (9), we argue by induction on $\#T$. If $\#T = 1$ then $T = 0$ and $z_0 = x_0y_0 = 0$. Let $p^r \leq p^{m+n}$ with $r \geq 1$ and assume by induction that for all $U < V$ such that $\#U < p^r$, $z_U \equiv 0 \bmod pR$. Pick $T \leq V$ with $\#T = p^r$. Since the T-th Witt polynomial is a multiplicative function $W_T\colon \mathbf{W}_G(R) \to R$, $W_T(\mathbf{z}) = W_T(\mathbf{x})W_T(\mathbf{y})$:

$$\sum_{U \leq T} \varphi_T(U) z_U^{\#T/\#U} = \sum_{T_1, T_2 \leq T} \varphi_T(T_1)\varphi_T(T_2) x_{T_1}^{\#T/\#T_1} y_{T_2}^{\#T/\#T_2}.$$

Solving this equation for z_T in $\mathbf{Q}[\underline{X}, \underline{Y}]$,

$$z_T = \sum_{T_1, T_2 \leq T} \frac{\varphi_T(T_1)\varphi_T(T_2)}{\varphi_T(T)} x_{T_1}^{\#T/\#T_1} y_{T_2}^{\#T/\#T_2} - \sum_{U < T} \frac{\varphi_T(U)}{\varphi_T(T)} z_U^{\#T/\#U}. \tag{10}$$

Since $z_U \in pR$ for $U < T$, the second term in (10) is 0 mod pR by Lemma 3.13. In the first term in (10), if $T_1 = V$ then $T_1 = T = V$ and $\varphi_T(T_1)\varphi_T(T_2)/\varphi_T(T) \equiv \varphi_T(T_2) \equiv 0 \bmod pR$ by Lemma 3.9 provided $T_2 \neq 0$, while if $T_2 = 0$ then $y_{T_2} = 0$. A similar argument holds if $T_2 = V$ so we can assume $T_1 < V$ and $T_2 < V$. If either $\#T_1 < p^m$ or $\#T_2 < p^n$ then $x_{T_1} = 0$ or $y_{T_2} = 0$ respectively. The remaining terms in the first sum in (10) have $T_1 < V$ with $\#T_1 \geq p^m$ and $T_2 < V$ with $\#T_2 \geq p^n$. In this case $\#T_1\#T_2 \geq p^{m+n} > p^r = \#T$, so by the ratio property the coefficient in the first sum in (10) is an integral multiple of p. Thus $z_T \equiv 0 \bmod pR$. □

Theorem 3.16. *Let G be a pro-p group. If it satisfies the ratio property, then for all rings A of characteristic p and nonnegative integers m and n,*

$$I_{p^m}(G, A) I_{p^n}(G, A) \subset I_{p^{m+n}}(G, A)$$

in $\mathbf{W}_G(A)$. In particular, this containment is true when G is abelian.

Proof. If either m or n is 0, since $I_1(G, A) = \mathbf{W}_G(A)$ the result follows. So we can assume $m > 0$ and $n > 0$. Let $\mathbf{a} \in I_{p^m}(G, A)$ and $\mathbf{b} \in I_{p^n}(G, A)$ and set $\mathbf{c} = \mathbf{ab}$. Let $V \in \mathcal{F}(G)$ such that $\#V < p^{m+n}$. Since $a_U = 0$ for all $\#U < p^m$ and $b_U = 0$ for all $\#U < p^n$, by Lemma 3.15 $c_V = 0$, so $\mathbf{c} \in I_{p^{m+n}}$. □

Remark 3.17. Of course the hypothesis that A has characteristic p is necessary, even in the classical case. Consider $G = \mathbf{Z}_p$. In $\mathbf{W}_G(\mathbf{Z})$, let $\mathbf{x} = (0, 1, 0, 0, \ldots) = \omega_{\mathbf{Z}_p/p\mathbf{Z}_p}(1)$. Clearly $\mathbf{x} \in I_p(G, \mathbf{Z})$ and from the proof of Theorem 6.1, $\mathbf{x}^2 = p\mathbf{x} = (0, p, \ldots)$, which is not in $I_{p^2}(G, \mathbf{Z})$.

A natural extension of the ratio property to arbitrary profinite groups G is the following: for all finite transitive G-sets T, T_1, and T_2 such that $T \geq T_1$, $T \geq T_2$, and $\#T$ is a proper factor of $\#T_1\#T_2$, the ratio $\varphi_T(T_1)\varphi_T(T_2)/\varphi_T(T)$ is an integer greater than 1. In this extra generality, which we don't need, there are counterexamples, specifically among symmetric and alternating groups.

No finite p-groups have been found yet which violate the ratio property. Even if a counterexample were to be found, a special case of Theorem 3.16 is nevertheless true for all p-groups.

Lemma 3.18. *Let G be a pro-p group. For all rings A of characteristic p and nonnegative integers n,*

$$I_p(G,A)I_{p^n}(G,A) \subset I_{p^{n+1}}(G,A)$$

in $\mathbf{W}_G(A)$.

Proof. If $n = 0$ the result is clear since $I_1(G,A) = \mathbf{W}_G(A)$, so without loss of generality assume $n \geq 1$.

We will derive a mod p congruence for particular Witt vectors over the ring $R = \mathbf{Z}[\underline{X}, \underline{Y}]$, which will be sufficient using functoriality. Define $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{W}_G(R)$ by

$$x_T = \begin{cases} 0, & \text{if } T = 0, \\ X_T, & \text{if } T \neq 0, \end{cases} \quad \text{and} \quad y_T = \begin{cases} 0, & \text{if } \#T < p^n, \\ Y_T, & \text{otherwise.} \end{cases}$$

Set $\mathbf{z} = \mathbf{xy}$. Our aim is to show

$$\#T < p^{n+1} \Longrightarrow z_T \equiv 0 \bmod pR. \tag{11}$$

We argue by induction on $\#T$. Clearly $z_0 = x_0 y_0 = 0$. Let $\#T = p^r < p^{n+1}$ with $r \geq 1$ and assume by induction that for all $\#U < p^r$, $z_U \equiv 0 \bmod pR$. Since the T-th Witt polynomial is a multiplicative function $W_T \colon \mathbf{W}_G(R) \to R$, $W_T(\mathbf{z}) = W_T(\mathbf{x})W_T(\mathbf{y})$:

$$\sum_{U \leq T} \varphi_T(U) z_U^{\#T/\#U} = \sum_{T_1, T_2 \leq T} \varphi_T(T_1)\varphi_T(T_2) x_{T_1}^{\#T/\#T_1} y_{T_2}^{\#T/\#T_2}.$$

Solving this equation for z_T in $\mathbf{Q}[\underline{X}, \underline{Y}]$,

$$z_T = \sum_{T_1, T_2 \leq T} \frac{\varphi_T(T_1)\varphi_T(T_2)}{\varphi_T(T)} x_{T_1}^{\#T/\#T_1} y_{T_2}^{\#T/\#T_2} - \sum_{U < T} \frac{\varphi_T(U)}{\varphi_T(T)} z_U^{\#T/\#U}. \tag{12}$$

Since $z_U \in pR$ for $U < T$, the second term in (12) is 0 mod pR by Lemma 3.13. In the first term in (12), we can assume $T_1 \neq 0$ since $x_0 = 0$. If $\#T_2 < p^n$ then $y_{T_2} = 0$, so we only need to consider T_2 where $\#T_2 \geq p^n$. Since $\#T < p^{n+1}$, $T_2 = T$. Then (12) becomes

$$z_T = \sum_{0 < T_1 \leq T} \varphi_T(T_1) x_{T_1}^{\#T/\#T_1} y_T - \sum_{U < T} \frac{\varphi_T(U)}{\varphi_T(T)} z_U^{\#T/\#U}.$$

Since $\varphi_T(T_1)$ is an integral multiple of p by Lemma 3.9, $z_T \equiv 0 \bmod pR$. □

An immediate useful corollary follows.

Corollary 3.19. *For any pro-p group G and ring A of characteristic p,*

$I_p(G,A)^m \subset I_{p^m}(G,A)$.

Proof. This follows directly from repeated applications of Lemma 3.18. □

Theorem 3.20. *Let G be a pro-p group and A be a ring of characteristic p. The units in $\mathbf{W}_G(A)$ are $\mathbf{W}_G(A)^\times = \{\mathbf{a} : a_0 \in A^\times\}$.*

Proof. Obviously $\mathbf{W}_G(A)^\times \subset \{\mathbf{a} : a_0 \in A^\times\}$. To prove the reverse inclusion, let $\mathbf{a} \in \mathbf{W}_G(A)$ have $a_0 \in A^\times$. By Theorem 2.10 the Witt vector $(a_0, 0, 0, \dots)$ is a unit, with inverse $(a_0^{-1}, 0, 0, \dots)$, so it suffices to show $(a_0^{-1}, 0, 0, \dots)\mathbf{a}$ is a unit. The first coordinate of this product is 1, so we are reduced to showing a Witt vector with first coordinate 1 is a unit. That is, we can assume $a_0 = 1$. By Theorem 2.8,

$$\mathbf{a} = (1, 0, 0, \dots) + (0, \{a_T\}_{T \neq 0}) \in 1 + I_p(G,A).$$

Since $I_p(G,A)^m \subset I_{p^m}(G,A)$ by Corollary 3.19, we can invert $\mathbf{a}$ using a geometric series since $\mathbf{W}_G(A)$ is complete in the initial vanishing topology (Theorem 3.5). □

Corollary 3.21. *When G is a pro-p group and A is a local ring of characteristic p, $\mathbf{W}_G(A)$ is a local ring. In particular, if k is a field of characteristic p then $\mathbf{W}_G(k)$ is a local ring.*

Proof. Let A have maximal ideal M. By Theorem 3.20, the complement of the unit group in $\mathbf{W}_G(A)$ is $\{\mathbf{a} \in \mathbf{W}_G(A) : a_0 \in M\}$, which is an ideal. □

The unique maximal ideal in $\mathbf{W}_G(k)$ for k is a field is easy to identify. We have a surjective homomorphism $\mathrm{Proj}^G_{G/G} : \mathbf{W}_G(k) \to \mathbf{W}_0(k) \cong k$. Therefore, the kernel $\mathfrak{m} = \{\mathbf{a} \in \mathbf{W}_G(k) : a_0 = 0\}$ is a maximal ideal in $\mathbf{W}_G(k)$. We also have $\mathfrak{m} = I_\ell$ where ℓ is the least integer greater than 1 such that G has an open subgroup of index ℓ (such an ℓ exists unless G is the trivial group). When G is a pro-p group and k a field of characteristic p, $\mathfrak{m} = I_p(G,k)$. In this setting we have three topologies: the $\mathfrak{m}$-adic topology, the initial vanishing (or $\{I_{p^n}\}$-adic) topology, and the profinite topology.

We have already compared the last two topologies in Theorem 3.7. By Corollary 3.19,

$$\mathfrak{m}^n = I_p(G,k)^n \subset I_{p^n}(G,k), \tag{13}$$

so $\bigcap_{n \geq 1} \mathfrak{m}^n = \{\mathbf{0}\}$, which shows the $\mathfrak{m}$-adic topology on $\mathbf{W}_G(k)$ is Hausdorff. Since $\mathfrak{m}^n \subset I_p^n \subset K_N$ for N any open normal subgroup such that $[G:N] > p^n$, open sets in the profinite topology are also open in the initial vanishing topology, which are open in the $\mathfrak{m}$-adic topology. It is not so clear how the higher powers of $\mathfrak{m}$ are related to the ideals I_{p^n} other than by (13). In the case of $\mathbf{W}_{\mathbf{Z}_p}(k)$ where k is a perfect field of characteristic p, i.e., the classical Witt vectors, the initial vanishing topology is the same as the $\mathfrak{m}$-adic topology since $\mathfrak{m} = (p) = I_p$ and $\mathfrak{m}^n = I_{p^n}$. Later, (Theorem 5.9) we will see for $G = \mathbf{Z}_p^d$ with $d \geq 2$ that the initial vanishing and $\mathfrak{m}$-adic topologies on $\mathbf{W}_G(k)$ are not the same.

4 The Frame of $\mathbf{Z}_p^d$

Throughout this section $G = \mathbf{Z}_p^d$ with $d \geq 2$ and a G-set will be finite transitive unless otherwise stated.

The subgroup structure of G is homogeneous in the sense that every open subgroup is isomorphic to G (although there is not a canonical choice of isomorphism, unlike the case when $d = 1$). A subgroup is open if and only if it has finite index. If H is an open subgroup there is a $\mathbf{Z}_p$-basis $\{e_1, e_2, \ldots, e_d\}$ for G such that $G = \mathbf{Z}_p e_1 \oplus \mathbf{Z}_p e_2 \oplus \cdots \oplus \mathbf{Z}_p e_d$ and $H = \mathbf{Z}_p p^{a_1} e_1 \oplus \mathbf{Z}_p p^{a_2} e_2 \oplus \cdots \oplus \mathbf{Z}_p p^{a_d} e_d$ for some $a_1, \ldots, a_d \geq 0$. The G-set G/H has the form

$$G/H \cong \mathbf{Z}_p/p^{a_1}\mathbf{Z}_p \times \mathbf{Z}_p/p^{a_2}\mathbf{Z}_p \times \cdots \times \mathbf{Z}_p/p^{a_d}\mathbf{Z}_p. \tag{14}$$

As a group, G/H is usually a product of d nontrivial cyclic p-groups. For some H, $a_i = 0$ for all but one i, making $T = G/H$ a cyclic group.

Definition 4.1. Let G be any profinite group and N be an open normal subgroup. A G-set $T \cong G/N$ where G/N is a cyclic group is called a *cyclic* G-set.

An important property about cyclic G-sets T when G is a pro-p group is that the G-sets $U < T$, which is called the *strict downset of* T, form a chain.

For $G = \mathbf{Z}_p^d$, from the large number of $\mathbf{Z}_p$-bases of G it is reasonable to expect that there are many cyclic G-sets of each size as the size grows. We will use cyclic G-sets later (Lemma 4.4) to find nonisomorphic G-sets of the same size with the same strict downsets, i.e., the G-sets lying below them in the frame of G are the same, which will be important in Section 5.

For each $T \in \mathcal{F}(G)$, there is an open subgroup $H \subset G$ with $T \cong G/H$, and H is uniquely determined by T since G is abelian: H is the common stabilizer of all points in T. Using a $\mathbf{Z}_p$-basis $\{e_1, e_2, \ldots, e_d\}$ of G we can identify H with $p^{a_1}\mathbf{Z}_p \times p^{a_2}\mathbf{Z}_p \times \cdots \times p^{a_d}\mathbf{Z}_p$ (this amounts to applying an automorphism of G), so the G-sets below G/H in $\mathcal{F}(G)$ are in one-to-one correspondence with the (open) subgroups of G that contain $p^{a_1}\mathbf{Z}_p \times p^{a_2}\mathbf{Z}_p \times \cdots \times p^{a_d}\mathbf{Z}_p$.

The frame of $\mathcal{F}(\mathbf{Z}_p)$ is linearly ordered so every element has a unique cover. Since every subgroup of $\mathbf{Z}_p^d$ is isomorphic to $\mathbf{Z}_p^d$ and there are $p^{d-1} + \ldots + p + 1$ maximal subgroups of $\mathbf{Z}_p^d$ the number of covers of each element of $\mathcal{F}(G)$ is the same.

Theorem 4.2. *Let $T \in \mathcal{F}(\mathbf{Z}_p^d)$. It has $p^{d-1}+\ldots+p+1$ covers in $\mathcal{F}(\mathbf{Z}_p^d)$ and in the case $T \geq \mathbf{Z}_p^d/p\mathbf{Z}_p^d$, it covers $p^{d-1} + \ldots + p + 1$ elements of $\mathcal{F}(\mathbf{Z}_p^d)$.*

Proof. Let H be the stabilizer of T. Covers of T correspond to subgroups of H with index p, which correspond to maximal subgroups of $H/pH \cong (\mathbf{Z}/p\mathbf{Z})^d$. By duality the number of such subgroups is the number of subgroups of H/pH with size p, namely the number of linear subspaces of $(\mathbf{Z}/p\mathbf{Z})^d$. That is $(p^d-1)/(p-1) = 1 + p + \ldots + p^{d-1}$.

Similarly, if T covers U then $U = \mathbf{Z}_p^d/K$ where $H \subset K$ and $[K : H] = p$, so the sets which T covers correspond to subgroups of size p in $\mathbf{Z}_p^d/H$. The number of such subgroups is the same as the number of subgroups of index p. When $\mathbf{Z}_p^d/H \geq \mathbf{Z}_p^d/p\mathbf{Z}_p^d$, we have $H \subset p\mathbf{Z}_p^d$. All subgroups of $\mathbf{Z}_p^d$ with index p contain $p\mathbf{Z}_p^d$, so the number of subgroups of index p in $\mathbf{Z}_p^d/H$ and $\mathbf{Z}_p^d/p\mathbf{Z}_p^d$ is the same.

□

In some calculations, it was noticed that many pairs of coordinates in sums or products of certain Witt vectors are equal. This is described formally by Lemmas 5.1 and 5.2 below and motivates the following definition.

Definition 4.3. A nonisomorphic pair of G-sets T and T', whose strict downsets agree, is called *linked.*

For a linked pair of G-sets T and T', $\#T = \#T'$ since for any $U < T$ of maximal size, $\#T = p\#U$. Therefore $\#T' = p\#U = \#T$. An example of such a pair T and T' is labeled in Figure 2. The pair V_1 and V_2 in Figure 2 is not linked since the G-set U_1 is below V_1 and not below V_2.

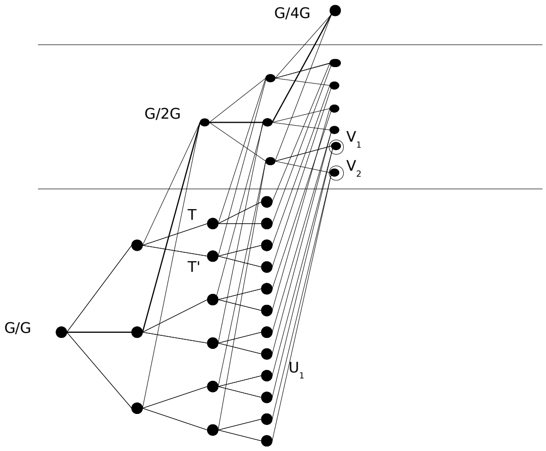

Figure 2: Linked and non-linked G-sets, $G = \mathbf{Z}_2^2$.

Our first task is to show that linked pairs of G-sets of arbitrarily large size exist for $G = \mathbf{Z}_p^d$ for $d \geq 2$. Of course, there are no linked $\mathbf{Z}_p$-sets.

Lemma 4.4. *For each $n \geq 1$ and cyclic G-set T of size p^{n-1}, there is a linked pair of cyclic G-sets T_1 and T_2 covering T.*

Proof. Since G is abelian, G-sets G/H for different (open) subgroups H are nonisomorphic. Since $d \geq 2$, there is more than one subgroup of index p. That settles the case $n = 1$.

Now let $n \geq 2$ and write $T = G/H$. There is a unique chain of subgroups

$$H = K_0 \subset K_1 \subset \cdots \subset K_{n-1} = G$$

where $[K_i : H] = p^i$ for all i.

There is a $\mathbf{Z}_p$-basis of $\mathbf{Z}_p^d$, $\{e_1, \ldots, e_d\}$, such that $H = \bigoplus_{i=1}^{d-1} \mathbf{Z}_p e_i \oplus \mathbf{Z}_p p^{n-1} e_d$. Consider the subgroups $H_1 = \bigoplus_{i=1}^{d-1} \mathbf{Z}_p e_i \oplus \mathbf{Z}_p p^n e_d$ and $H_2 = \bigoplus_{i=1}^{d-2} \mathbf{Z}_p e_i \oplus \mathbf{Z}_p p e_{d-1} \oplus \mathbf{Z}_p(e_{d-1} + p^{n-1} e_d)$. Clearly $H_1 \subset H$ and $H_2 \subset H$ and both G/H_1 and G/H_2 are cyclic. Since $\#G/H_1$ and $\#G/H_2$ are both p^n, G/H_1 and G/H_2 are covers of G/H.

Set $T_1 = G/H_1$ and $T_2 = G/H_2$. Since $H_1 \neq H_2$, T_1 and T_2 are nonisomorphic. To show their strict downsets agree, we use the cyclic condition. The G-sets $U < T_1$ are G/K_i for $i = 0, \ldots, n-1$. The same argument applies to T_2, so the same G-sets lie strictly below T_1 and T_2 in the frame of G. □

5 Non-finitely generated ideals $\mathbf{W}_{\mathbf{Z}_p^d}(k)$

When k is a perfect field of characteristic p and $d \geq 2$, one might expect the rings $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ generalize the classical Witt vectors $\mathbf{W}_{\mathbf{Z}_p}(k)$ in the same way that $k[[X_1, \ldots, X_d]]$ generalizes $k[[X_1]]$: the power series ring in d variables over a field is a complete local Noetherian domain with dimension d. We will see in Theorem 6.1 that $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is not a domain whether or not k is perfect. On the positive side, $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is a local ring (Corollary 3.21), whether or not k is perfect, and it is complete with respect to the initial vanishing topology (Theorem 3.5) which is the same as the profinite topology since $\mathbf{Z}_p^d$ is topologically finitely generated (Theorem 3.7). It is plausible to guess, by analogy to $k[[X_1, \ldots, X_d]]$, that the maximal ideal of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is generated by the Witt vectors $\omega_T(1)$ for $\#T = p$, but we will see this is false in a very strong way: $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is not Noetherian, whether or not k is perfect. This is because, as we will see, the square of the maximal ideal of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is much smaller than intuition suggests.

5.1 $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is not Noetherian for $d \geq 2$

To prove $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ is not Noetherian, we use Lemma 4.4 to prove two lemmas below that describe different coordinates that are equal in a sum and product of suitable Witt vectors. The upshot, Theorem 5.4, is that Witt vectors in the square of the maximal ideal of $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ have built-in redundancies in linked coordinates which occur arbitrarily far out into the frame of $\mathbf{Z}_p^d$ when $d \geq 2$.

We continue to use the convention that G stands for $\mathbf{Z}_p^d$.

Lemma 5.1. *Let A be a ring. Given linked G-sets T and T' and a finite collection of Witt vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m \in \mathbf{W}_G(A)$ such that $(\mathbf{a}_i)_T = (\mathbf{a}_i)_{T'}$ for $1 \leq i \leq m$, set $\mathbf{s} = \sum\limits_{i=1}^{m} \mathbf{a}_i$. Then $s_T = s_{T'}$.*

Proof. By induction it suffices to check the case $m = 2$.

Since T and T' are linked i.e., the G-sets strictly below T and T' in $\mathcal{F}(G)$ are the same, $\#T = \#T'$ and the Witt polynomials $W_T(\underline{X})$ and $W_{T'}(\underline{X})$ are the same up to the roles of X_T, Y_T and $X_{T'}, Y_{T'}$ in them. Therefore the two sum polynomials S_T and $S_{T'}$ are the same up to the roles of X_T, Y_T, $X_{T'}$, and $Y_{T'}$ in them (and we know how X_T, Y_T, $X_{T'}$ and $Y_{T'}$ appear in S_T and $S_{T'}$ by Theorem 2.11). So when Witt vectors $\mathbf{a}_1$ and $\mathbf{a}_2$ have the same T and T' coordinates, since T and T' are linked we have $S_T(\mathbf{a}_1, \mathbf{a}_2) = S_{T'}(\mathbf{a}_1, \mathbf{a}_2)$. Thus $(\mathbf{a}_1 + \mathbf{a}_2)_T = (\mathbf{a}_1 + \mathbf{a}_2)_{T'}$.

For a second argument, let $R = \mathbf{Z}[\underline{X}, \underline{Y}]$ and choose Witt vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{W}_G(R)$ with $x_U = X_U$ and $y_U = Y_U$ for all $U \neq T'$, $x_{T'} = X_T$, and $y_{T'} = Y_T$. These are "generic" Witt vectors with equal coordinates at T and T'. We will show for $\mathbf{z} = \mathbf{x} + \mathbf{y}$ that $\mathbf{z}_T = \mathbf{z}_{T'}$. The lemma will then follow by functoriality.

The T-th Witt polynomial has the form

$$W_T(\underline{X}) = \sum_{U \leq T} \#U X_U^{\#T/\#U}.$$

Consider the equations $W_T(\mathbf{z}) = W_T(\mathbf{x}) + W_T(\mathbf{y})$ and $W_{T'}(\mathbf{z}) = W_{T'}(\mathbf{x}) + W_{T'}(\mathbf{y})$. Writing these equations out,

$$\sum_{U \leq T} \#U z_U^{\#T/\#U} = \sum_{U \leq T} \#U (x_U^{\#T/\#U} + y_U^{\#T/\#U}) \tag{15}$$

and

$$\sum_{U \leq T'} \#U z_U^{\#T'/\#U} = \sum_{U \leq T'} \#U (x_U^{\#T'/\#U} + y_U^{\#T'/\#U}). \tag{16}$$

Since T and T' are linked, $\#T = \#T'$ and $\{U < T\} = \{U < T'\}$, so after subtracting (16) from (15) we get $\#T(z_T - z_{T'}) = \#T(x_T - x_{T'} + y_T - y_{T'}) = 0$ in R, which gives $z_T = z_{T'}$, as desired. □

Unlike the previous lemma, the next one is specific to rings of characteristic p.

Lemma 5.2. *Let A be a ring of characteristic p. Given a pair of linked G-sets T and T' and elements $\mathbf{a}$ and $\mathbf{b}$ of $\mathbf{W}_G(A)$ such that $a_0 = b_0 = 0$, the product $\mathbf{m} = \mathbf{ab}$ satisfies $m_T = m_{T'}$.*

Proof. Let $R = \mathbf{Z}[\underline{X}, \underline{Y}]$ and define $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{W}_G(R)$ by $x_U = X_U$ and $y_U = Y_U$ for all U. Set $\mathbf{z} = \mathbf{xy}$. We will show

$$z_T - z_{T'} \equiv (x_T - x_{T'}) y_0^{p^n} + (y_T - y_{T'}) x_0^{p^n} \bmod pR.$$

Since A has characteristic p, it would then follow by functoriality that $\mathbf{ab}$ has equal T and T' coordinates in $\mathbf{W}_G(A)$.

Since the T-th Witt polynomial is a multiplicative function $W_T\colon \mathbf{W}_G(R) \to R$, $W_T(\mathbf{z}) = W_T(\mathbf{x})W_T(\mathbf{y})$:

$$\sum_{U \le T} \#U z_U^{\#T/\#U} = \left(\sum_{U\le T} \#U x_U^{\#T/\#U}\right)\left(\sum_{U\le T} \#U y_U^{\#T/\#U}\right).$$

Isolating the z_T term,

$$\#T z_T = \left(\sum_{U\le T} \#U x_U^{\#T/\#U}\right)\left(\sum_{U\le T} \#U y_U^{\#T/\#U}\right) - \sum_{U<T} \#U z_U^{\#T/\#U}. \tag{17}$$

Likewise looking at the T' coordinate we have

$$\#T' z_{T'} = \left(\sum_{U\le T'} \#U x_U^{\#T'/\#U}\right)\left(\sum_{U\le T'} \#U y_U^{\#T'/\#U}\right) - \sum_{U<T'} \#U z_U^{\#T'/\#U}. \tag{18}$$

Since T and T' are linked, $\#T = \#T'$ and $\{U < T\} = \{U < T'\}$ so the z-terms being subtracted on the right side of (17) and (18) are the same. Subtracting (18) from (17) and setting $\#T = \#T' = p^n$, we have

$$\begin{aligned}
p^n z_T - p^n z_{T'} &= \left(\sum_{U\le T} \#U x_U^{\frac{p^n}{\#U}}\right)\left(\sum_{U\le T} \#U y_U^{\frac{p^n}{\#U}}\right) - \sum_{U<T} \#U z_U^{\frac{p^n}{\#U}} \\
&\quad - \left(\sum_{U\le T'} \#U x_U^{\frac{p^n}{\#U}}\right)\left(\sum_{U\le T'} \#U y_U^{\frac{p^n}{\#U}}\right) + \sum_{U<T'} \#U z_U^{\frac{p^n}{\#U}} \\
&= p^{2n} x_T y_T + p^n x_T \sum_{U<T} \#U y_U^{\frac{p^n}{\#U}} + p^n y_T \sum_{U<T} \#U x_U^{\frac{p^n}{\#U}} \\
&\quad -p^{2n} x_{T'} y_{T'} - p^n x_{T'} \sum_{U<T'} \#U y_U^{\frac{p^n}{\#U}} - p^n y_{T'} \sum_{U<T'} \#U x_U^{\frac{p^n}{\#U}} \\
&\equiv p^n x_T y_0^{p^n} + p^n x_0^{p^n} y_T - p^n x_{T'} y_0^{p^n} - p^n x_0^{p^n} y_{T'} \bmod p^{n+1}R \\
&\equiv p^n (x_T y_0^{p^n} + x_0^{p^n} y_T - x_{T'} y_0^{p^n} - x_0^{p^n} y_{T'}) \bmod p^{n+1}R \\
&\equiv p^n ((x_T - x_{T'}) y_0^{p^n} + (y_T - y_{T'}) x_0^{p^n}) \bmod p^{n+1}R.
\end{aligned}$$

So $z_T - z_{T'} \equiv (x_T - x_{T'}) y_0^{p^n} + (y_T - y_{T'}) x_0^{p^n} \bmod pR$. □

Remark 5.3. The characteristic p hypothesis in Lemma 5.2 is necessary. Consider the case $G = \mathbf{Z}_p^d$ for $d \ge 2$ and $\mathbf{W}_G(\mathbf{Z})$. Any pair of nonisomorphic G-sets of size p is linked. Given two vectors $\mathbf{a}, \mathbf{b} \in \mathbf{W}_G(\mathbf{Z})$ such that $a_0 = b_0 = 0$, set $\mathbf{m} = \mathbf{ab}$. For $T \in \mathcal{F}(G)$ such that $\#T = p$, the formula for M_T in Example 2.5 implies $m_T = pa_Tb_T$, which depends on T for suitable choices of $\mathbf{a}$ and $\mathbf{b}$.

The point of these last two lemmas is that for linked G-sets T and T', the T and T' coordinates of a sum are the same if we make an assumption about the T and T' coordinates of the summands, while the T and T' coordinates of a product are the same if we make an assumption about the coordinates of the factors at the trivial G-set.

Let k be a field of characteristic p. For $n \geq 0$, recall the notation

$$I_{p^n} = I_{p^n}(G,k) = I_{p^n}(\mathbf{Z}_p^d, k) = \{\mathbf{a} \in \mathbf{W}_{\mathbf{Z}_p^d}(k); a_T = 0 \text{ if } \#T < p^n\}.$$

The unique maximal ideal of $\mathbf{W}_G(k)$ is $\mathfrak{m} = I_p(G,k)$.

Theorem 5.4. *Let T and T' be linked G-sets. Any element of $\mathfrak{m}^2$ has equal T and T' coordinates.*

Proof. Any element of $\mathfrak{m}^2$ is $\mathbf{a}_1\mathbf{b}_1 + \cdots + \mathbf{a}_r\mathbf{b}_r$ for some $\mathbf{a}_i$ and $\mathbf{b}_i$ in $\mathfrak{m}$. Lemma 5.2 shows that $\mathbf{a}_i\mathbf{b}_i$ has the same T and T' coordinates for all i. Applying Lemma 5.1 shows that this equality of coordinates is preserved when passing to the sum of these products over all i. □

Since Lemma 4.4 shows that there are linked G-sets of arbitrarily large size, Theorem 5.4 puts infinitely many constraints on elements of $\mathfrak{m}^2$. Theorem 5.4 was first observed in examples, where many redundancies were noticed in different coordinates of a product of elements of $\mathbf{W}_{\mathbf{Z}_2^2}(\mathbf{F}_2[\underline{X}, \underline{Y}])$ that each have first coordinate 0. This is also how the importance of linked G-sets was discovered. We are now set to use them to prove our first main structural theorem.

Lemma 5.5. *Let k be a field of characteristic p and $\mathfrak{m}$ be the unique maximal ideal of $\mathbf{W}_G(k)$. Then* $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \infty$.

Theorem 5.6. *The maximal ideal of $\mathbf{W}_G(k)$ is not finitely generated, so $\mathbf{W}_G(k)$ is not Noetherian.*

Proof. Using Lemma 4.4, for each $n \geq 1$ there are linked G-sets T_n and T'_n in $\mathcal{F}(G)$ of size p^n. In particular, $\{U : U < T_n\} = \{U : U < T'_n\}$. The Witt vector $\omega_{T_n}(1)$ lies in $\mathfrak{m}$. For each $r \geq 1$ we will show the r Witt vectors $\omega_{T_1}(1), \ldots, \omega_{T_r}(1)$ are linearly independent over k in $\mathfrak{m}/\mathfrak{m}^2$.

In $\mathfrak{m}/\mathfrak{m}^2$, suppose we have a k-linear relation

$$\alpha_1\omega_{T_1}(1) + \cdots + \alpha_r\omega_{T_r}(1) \equiv 0 \bmod \mathfrak{m}^2,$$

for some $\alpha_i \in k$. The product $\alpha_i\omega_{T_i}(1)$ in $\mathfrak{m}/\mathfrak{m}^2$ really means, as a Witt vector, $\omega_0(\alpha_i)\omega_{T_i}(1)$ mod $\mathfrak{m}^2$. By Theorem 2.10, $\omega_0(\alpha_i)\omega_{T_i}(1) = \omega_{T_i}(\alpha_i^{p^i})$. Therefore

$$\omega_{T_1}(\alpha_1^p) + \cdots + \omega_{T_r}(\alpha_r^{p^r}) \equiv 0 \bmod \mathfrak{m}^2. \tag{19}$$

Since the supports of $\omega_{T_i}(\alpha_i^{p^i})$ for $1 \leq i \leq r$ are disjoint, by Theorem 2.8 these Witt vectors can be added coordinatewise: the left side of (19) is the Witt vector with T_i-coordinate $\alpha_i^{p^i}$ and other coordinates equal to 0. Since this sum is in $\mathfrak{m}^2$, its T_i- and T_i'-coordinates are the same by Theorem 5.4. The T_i'-coordinate is 0 for all i, so $\alpha_i^{p^i} = 0$ for all i. Thus every α_i is 0 in k.

Since we have found r linearly independent elements of $\mathfrak{m}/\mathfrak{m}^2$ for any $r \geq 1$, its k-dimension is infinite.

A finite set of generators of $\mathfrak{m}$ would span $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space. We have just shown that no such set can exist, so $\mathfrak{m}$ is not finitely generated. Hence $\mathbf{W}_G(A)$ is not Noetherian. □

Corollary 5.7. *If A is a ring of characteristic p then $\mathbf{W}_G(A)$ is not Noetherian.*

Proof. For any maximal ideal M in A, the ring $\mathbf{W}_G(A/M)$ is not Noetherian by Theorem 5.6 and it is a quotient ring of $\mathbf{W}_G(A)$ by functoriality. □

Remark 5.8. For an infinite pro-p group G with arbitrarily large pairs of linked normal G-sets, the results of this section go through. For such pro-p groups, $\mathbf{W}_G(k)$ is not Noetherian when k is a field (or ring) of characteristic p.

As another application of Theorem 5.4, we compare the $\mathfrak{m}$-adic and initial vanishing topologies on $\mathbf{W}_G(k)$. From Corollary 3.19, $\mathfrak{m}^n \subset I_{p^n}$ for all n, so every I_{p^n} is open in the $\mathfrak{m}$-adic topology on $\mathbf{W}_G(k)$. Of course $\mathfrak{m}$ is open in the initial vanishing topology (defined by the ideals I_{p^n}) since $\mathfrak{m} = I_p$. We are going to show for $s \geq 2$ that $\mathfrak{m}^s$ is not open in the initial vanishing topology.

Theorem 5.9. *For each $s \geq 2$, the ideal $\mathfrak{m}^s$ in $\mathbf{W}_G(k)$ does not contain any I_{p^r}.*

Proof. Since $\mathfrak{m}^s \subset \mathfrak{m}^2$ for $s \geq 2$, it suffices to show $\mathfrak{m}^2$ contains no I_{p^r} for $r \geq 1$. For any $n \geq r$, there are linked G-sets T_n and T_n' of size p^n by Lemma 4.4. Then $\omega_{T_n}(1) \in I_{p^r}$ and by Theorem 5.4 $\omega_{T_n}(1) \notin \mathfrak{m}^2$, so $I_{p^r} \not\subset \mathfrak{m}^2$. □

5.2 $\mathbf{W}_{\mathbf{Z}_p^2}(k)$ is not coherent

Our next goal is to show for $G = \mathbf{Z}_p^2$ and p odd that $\mathbf{W}_G(k)$ is not coherent; a finiteness condition weaker than being Noetherian. We will need to keep track of a new partial ordering on $\mathcal{F}(G)$. This new partial ordering makes sense with no extra effort for $G = \mathbf{Z}_p^d$ with any $d \geq 1$ so we will state it in this generality. Consider the descending subgroup filtration

$$G \supsetneqq pG \supsetneqq p^2G \supsetneqq \cdots \supsetneqq p^nG \supsetneqq p^{n+1}G \supsetneqq \cdots,$$

which leads to the rising family of G-sets

$$0 = G/G < G/pG < G/p^2G < \cdots < G/p^nG < G/p^{n+1}G < \cdots$$

in $\mathcal{F}(G)$.

Definition 5.10. For $G = \mathbf{Z}_p^d$, the *level* of $T \in \mathcal{F}(G)$ is the largest $n \geq 0$ such that $T \geq G/p^nG$. We write $\mathrm{Lev}(T) = n$.

This definition makes sense, since if $T \geq G/p^nG$ then $\#T \geq p^{nd}$, so n is bounded above, and $T \geq 0$ so we have somewhere to begin. To get a feel for this concept, we describe it on coset spaces. Write $T \cong G/H$ for a unique open subgroup H of G. We have $T \geq G/p^nG$ if and only if $H \subset p^nG$. Therefore $\mathrm{Lev}(G/H)$ is the largest $n \geq 0$ such that $H \subset p^nG$. See Figure 3.

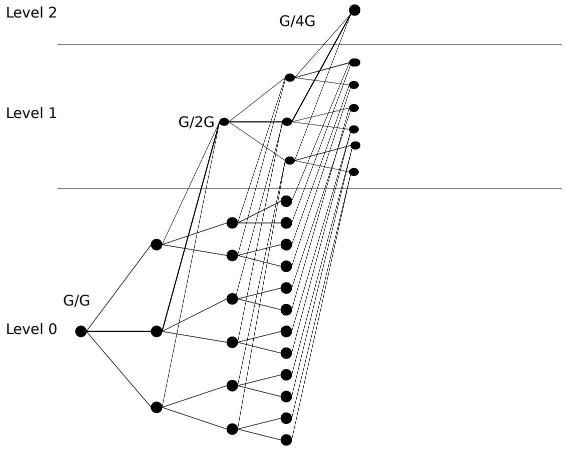

Figure 3: Initial G-sets of Level $0, 1, 2$ in $\mathcal{F}(G)$ for $G = \mathbf{Z}_2^2$.

If $G = \mathbf{Z}_p$ then $\mathrm{Lev}(T)$ and $\#T$ are basically the same concept, since $\#T = p^{\mathrm{Lev}(T)}$. The level is something genuinely new when $G = \mathbf{Z}_p^d$ for $d \geq 2$. In this case neither $\#T$ nor $\mathrm{Lev}(T)$ determines the other; all we can say in general is that $\#T \geq p^{d\,\mathrm{Lev}(T)}$.

Writing the cyclic decomposition of G/H as $\mathbf{Z}/p^{a_1}\mathbf{Z} \times \mathbf{Z}/p^{a_2}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{a_d}\mathbf{Z}$, its level is $\min\{a_1, a_2, \ldots, a_d\}$. This makes it easy to produce examples.

Example 5.11. For $a \geq 1$, the G-set $\mathbf{Z}_p^d/(\mathbf{Z}_p \times p^a\mathbf{Z}_p^{d-1})$ of size $p^{a(d-1)}$ has level 0 since $\mathbf{Z}_p \times p^a\mathbf{Z}_p^{d-1}$ is contained in G but not pG. So when $d \geq 2$, arbitrarily large G-sets can have level 0 (but not when $d = 1$).

Example 5.12. There are arbitrarily large G-sets of any chosen level n when $d \geq 2$: use $\mathbf{Z}_p^d/(p^n\mathbf{Z}_p \times p^{a+n}\mathbf{Z}_p^{d-1})$ with $a \to \infty$.

Theorem 5.13. *For $d \geq 2$, each $\mathbf{Z}_p^d$-set of level n is covered by more than one G-set of level n.*

Proof. Let T be a G-set with $\mathrm{Lev}(T) = n$. Pick a $\mathbf{Z}_p$-basis $\{e_1, \ldots, e_d\}$ of $\mathbf{Z}_p^d$ so that $T \cong G/H$ with $H = \mathbf{Z}_p p^{a_1}e_1 + \ldots + \mathbf{Z}_p p^{a_d}e_d$, where $n = a_1 \leq a_2 \leq \ldots \leq a_d$. When $d \geq 3$, $\sum_{i=1}^{d} \mathbf{Z}_p p^{a_i}e_i + \mathbf{Z}_p p^{a_d+1}e_d$ and $\sum_{i \neq d-1} \mathbf{Z}_p p^{a_i}e_i + \mathbf{Z}_p p^{a_{d-1}+1}e_{d-1}$ are subgroups of H with index p and they are the stabilizers of two distinct G-sets covering T both with level n. If $d = 2$, on the other hand, $\mathbf{Z}_p p^{a_1} e_1 + \mathbf{Z}_p p^{a_2+1} e_2$ and $\mathbf{Z}_p(p^{a_1+1}e_1 + p^{a_1}e_2) + \mathbf{Z}_p p^{a_2} e_2$ are subgroups of H with index p and they are the stabilizers of two distinct $\mathbf{Z}_p^2$-sets covering T both with level n. □

For any $T \in \mathcal{F}(G)$, $\{U : \#U \leq \#T\}$ and $\{U : U \leq T\}$ are finite (the latter is a subset of the former), but $\{U : \mathrm{Lev}(U) \leq \mathrm{Lev}(T)\}$ is infinite. This is an important distinction to remember.

Remark 5.14. When $d \geq 2$, any nontrivial cyclic G-set looks like $\mathbf{Z}_p^d/(\mathbf{Z}_p^{d-1} \times p^a\mathbf{Z}_p)$ with $a \geq 1$ after a suitable choice of basis for $\mathbf{Z}_p^d$, and $\mathbf{Z}_p^{d-1} \times p^a \mathbf{Z}_p$ is not contained in $p\mathbf{Z}_p^d$ (this is false for $d = 1$), so all cyclic G-sets have level 0. When $d = 2$, a G-set of level 0 is isomorphic to $\mathbf{Z}_p^2/(\mathbf{Z}_p \times p^a\mathbf{Z}_p)$, so level 0 and cyclic in $\mathcal{F}(\mathbf{Z}_p^2)$ mean the same thing. For $d \geq 3$, some G-sets of level 0 are not cyclic, such as $\mathbf{Z}_p^d/(\mathbf{Z}_p \times p\mathbf{Z}_p \times p^a\mathbf{Z}_p^{d-2})$ with $a \geq 1$.

A commutative ring A is called coherent provided that whenever $I \subset A$ is a finitely generated ideal, there are free A-modules A^m and A^n fitting into an exact sequence $A^m \to A^n \to I \to 0$. A necessary condition [3, p. 95] for A to be coherent is that the annihilators $\mathrm{Ann}(x) = \{a \in A : ax = 0\}$ for each $x \in A$ are finitely generated. We will show that $\mathbf{W}_G(k)$ does not satisfy this necessary condition when $G = \mathbf{Z}_p^2$ and p is odd. *For the rest of this subsection $G = \mathbf{Z}_p^2$ unless otherwise stated.*

Fix a G-set V such that $\#V = p$. We will show the annihilator $\mathrm{Ann}_V = \{\mathbf{w} \in \mathbf{W}_G(k) : \mathbf{w}\omega_V(1) = \mathbf{0}\}$ is not a finitely generated ideal. Pick a different G-set W also with $\#W = p$. Such a choice is possible since there is more than one maximal subgroup of G. We will describe a collection of G-sets $\{T_j, T_j'\}_{j \geq 2}$ such that

- T_j and T_j' are cyclic with size p^j,
- $W \leq T_j$ and $W \leq T_j'$, and
- for $j \geq 3$, both T_j and T_j' cover T_{j-1}.

It follows that T_j and T_j' are linked. To make this construction explicit, write $W = G/H_W$ and choose a $\mathbf{Z}_p$-basis $\{e_1, e_2\}$ for G such that $H_W = \mathbf{Z}_p e_1 \oplus \mathbf{Z}_p p e_2$. So in this basis $H_W = M_W(\mathbf{Z}_p^2)$, where $M_W = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$.

Define $T_j = G/H_j$ where $H_j = M_j(\mathbf{Z}_p^2)$ for $M_j = \begin{pmatrix} 1 & 0 \\ 0 & p^j \end{pmatrix}$. Likewise define $T_j' = G/H_j'$ where $H_j' = M_j'(\mathbf{Z}_p^2)$ for $M_j' = \begin{pmatrix} p & 1 \\ 0 & p^{j-1} \end{pmatrix}$.

Figure 4 is part of the diagram[1] for $\mathcal{F}(\mathbf{Z}_3^2)$ with V, W and T_j and T_j' labeled for $j = 2$ and 3.

Now we can make a precise statement about the G-sets which lie above the G-sets T_j or T_j'.

Lemma 5.15. *Let T be a G-set with* $\mathrm{Lev}(T) > 0$*. For each $j \geq 2$, if T lies above one of T_j or T_j' then it lies above the other one also.*

[1] Some covering relations were not drawn to preserve readability.

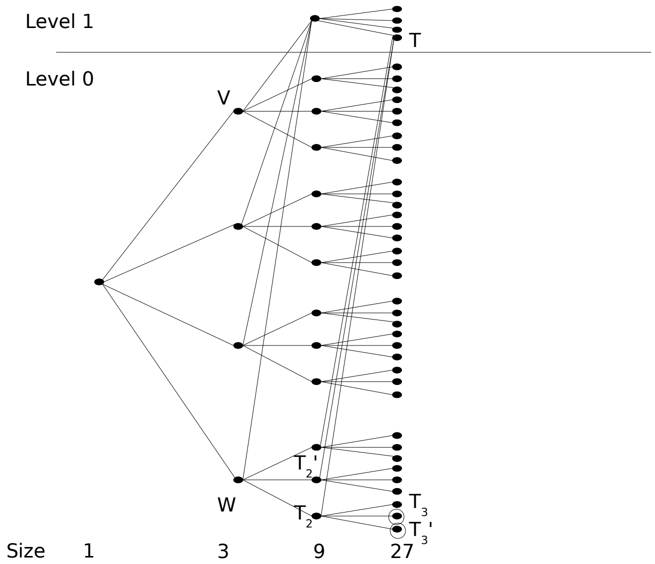

Figure 4: Portion of the frame $\mathcal{F}(G)$ where $G = \mathbf{Z}_3^2$.

Proof. Recall we have already chosen a $\mathbf{Z}_p$-basis $\{e_1, e_2\}$ of $\mathbf{Z}_p^2$ so that in that basis $T_j = G/H_j$ where $H_j = M_j(\mathbf{Z}_p^2)$ for $M_j = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p^j \end{smallmatrix}\right)$ and $T_j' = G/H_j'$ where $H_j' = M_j'(\mathbf{Z}_p^2)$ for $M_j' = \left(\begin{smallmatrix} p & 1 \\ 0 & p^{j-1} \end{smallmatrix}\right)$.

Using Hermite normal form, an arbitrary G-set T with $\mathrm{Lev}(T) > 0$ is isomorphic to G/H where $H = M_H(\mathbf{Z}_p^2)$ for $M_H = \left(\begin{smallmatrix} p^r & b \\ 0 & p^s \end{smallmatrix}\right)$ and $r \geq 2, s \geq 1$, $1 \leq b < p^r$ and $p|b$. The conclusion of the lemma is equivalent to the statement that whenever $H \subset H_j$ then $H \subset H_j'$ also, and vice versa. Notice that $H \subset H_j$ if and only if $M_j^{-1} M_H \in \mathrm{Mat}_2(\mathbf{Z}_p)$. Since $M_j^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p^{-j} \end{smallmatrix}\right)$, $M_j^{-1} M_H = \left(\begin{smallmatrix} p^r & b \\ 0 & p^{s-j} \end{smallmatrix}\right)$ and $H \subset H_j$ if and only if $s \geq j$. Also $M_j'^{-1} = \left(\begin{smallmatrix} p^{-1} & -p^{-j} \\ 0 & p^{1-j} \end{smallmatrix}\right)$, so $M_j'^{-1} M_H = \begin{pmatrix} p^{r-1} & \frac{b}{p} - \frac{p^s}{p^j} \\ 0 & p\frac{p^s}{p^j} \end{pmatrix}$. That $p^{r-1} \in \mathbf{Z}_p$ is automatic and since $p|b$, $b/p \in \mathbf{Z}_p$. So, $M_j'^{-1} M_H$ is in $\mathrm{Mat}_2(\mathbf{Z}_p)$ if and only if $p^s/p^j \in \mathbf{Z}_p$, or equivalently $s \geq j$. Since the conditions for $H \subset H_j$ or $H \subset H_j'$ are the same, assuming either inclusion guarantees the other. □

Our aim is to show that Ann_V is not finitely generated. We will do this using a subset N_V of Ann_V that is defined in the next lemma.

Lemma 5.16. *Let p be odd. The subset*

$$N_V = \{\mathbf{a} \in \mathbf{W}_G(k) : a_{T_j} + a_{T_j'} = 0 \text{ and } a_U = 0 \text{ for } U \notin \{T_j, T_j'\}_{j \geq 2}\}$$

is contained in Ann_V*: if $\mathbf{a} \in N_V$ then $\mathbf{a}\omega_V(1) = \mathbf{0}$.*

Proof. Let $R = \mathbf{Z}[\underline{X}]$ and $\mathbf{x}$ be the Witt vector in $\mathbf{W}_G(R)$ such that $x_U = 0$ for $U \notin \{T_j, T_j'\}_{j\geq 2}$, $x_{T_j} = X_{T_j}$, and $x_{T_j'} = -X_{T_j}$ for $j \geq 2$. Every $\mathbf{a} \in N_V$ is the image of $\mathbf{x}$ under a ring homomorphism $\mathbf{W}_G(R) \to \mathbf{W}_G(k)$. Let $\mathbf{v} = \omega_V(1)$ in $\mathbf{W}_G(R)$. Set $\mathbf{m} = \mathbf{vx}$. To prove the lemma it suffices to show $m_T \equiv 0 \bmod pR$ for all $T \in \mathcal{F}(G)$. In fact we will show $m_T = 0$. To show each coordinate of $\mathbf{m}$ is zero it suffices to show $W_T(\mathbf{m}) = 0$ for each $T \in \mathcal{F}(G)$ by Theorem 2.2. Clearly $m_0 = v_0x_0 = 0$. By direct computation, $W_T(\mathbf{v}) = p$ if $T \geq V$ and $W_T(\mathbf{v}) = 0$ otherwise. Therefore $W_T(\mathbf{m}) = W_T(\mathbf{v})W_T(\mathbf{x}) = 0$ for all T such that $V \not\leq T$.

Let $T \in \mathcal{F}(G)$ such that $V \leq T$. Assume $\mathrm{Lev}(T) = 0$ and consider the equation $W_T(\mathbf{m}) = W_T(\mathbf{v})W_T(\mathbf{x})$. Recall the distinguished G-set $W \neq V$ with $\#W = p$ and $W \leq T_j$ and $W \leq T_j'$. Since $G = \mathbf{Z}_p^2$ and $\mathrm{Lev}(T) = 0$, T is a cyclic G-set, so from $V \leq T$ we get $W \not\leq T$. Therefore $T_j \not\leq T$ and $T_j' \not\leq T$ for $j \geq 2$. Since T_j and T_j' for all $j \geq 2$ are the support of $\mathbf{x}$, $W_T(\mathbf{x}) = 0$. Thus $W_T(\mathbf{m}) = W_T(\mathbf{v})W_T(\mathbf{x}) = 0$ for each G-set T such that $\mathrm{Lev}(T) = 0$.

Now consider $\mathrm{Lev}(T) \geq 1$ with $V \leq T$. Set $\#T = p^n$. Clearly if none of the G-sets T_j nor T_j' for $j \geq 2$ lie below T then $W_T(\mathbf{x}) = 0$ and so $W_T(\mathbf{m}) = W_T(\mathbf{v})W_T(\mathbf{x}) = 0$. We may now assume $T_j \leq T$ or $T_j' \leq T$ for some $j \geq 2$. By Lemma 5.15, if T_j or T_j' is below T then both are. Set $r = \max\{j : T_j \leq T\} \geq 2$, so $T_j \leq T$ and $T_j' \leq T$ for all $j \in \{2, \ldots, r\}$. Now consider the equation

$$\begin{aligned}
W_T(\mathbf{m}) &= W_T(\mathbf{v})W_T(\mathbf{x}) \\
&= pW_T(\mathbf{x}) \\
&= p\sum_{U\leq T} \#U x_U^{\#T/\#U} \\
&= p\sum_{j=2}^{r} \#T_j x_{T_j}^{\#T/\#T_j} + \#T_j' x_{T_j'}^{\#T/\#T_j'} \\
&= \sum_{j=2}^{r} p^{j+1}(x_{T_j}^{p^{n-j}} + x_{T_j'}^{p^{n-j}}),
\end{aligned}$$

where the last equality comes from the fact that $\#T = p^n$ and $\#T_j = \#T_j' = p^j$. From the definition of $\mathbf{x}$ and p being odd, $x_{T_j}^{p^{n-j}} + x_{T_j'}^{p^{n-j}} = X_{T_j}^{p^{n-j}} - X_{T_j}^{p^{n-j}} = 0$. Therefore $W_T(\mathbf{m}) = 0$. □

Vectors in a finitely generated ideal $(\mathbf{b}_1, \ldots, \mathbf{b}_r)$ are finite sums $\sum_{i=1}^r \mathbf{b}_i\mathbf{c}_i$, where $\mathbf{c}_i \in \mathbf{W}_G(k)$. When each $\mathbf{b}_i$ is in $\mathfrak{m}$, we will derive a universal formula for selected coordinates in $\mathbf{b}_i\mathbf{c}_i$ and then for $\sum_{i=1}^r \mathbf{b}_i\mathbf{c}_i$. The coordinates are in characteristic p; by "universal formula" we really mean a mod p congruence involving selected Witt vectors over a polynomial ring over $\mathbf{Z}$. Functoriality will turn such formulas into formulas in $\mathbf{W}_G(k)$.

Lemma 5.17. *Let $R = \mathbf{Z}[\underline{X}, \underline{Y}]$ and $\mathbf{x}$ and $\mathbf{y}$ be the Witt vectors in $\mathbf{W}_G(R)$ with $x_0 = 0$, $x_U = X_U$*

for $U \neq 0$ and $y_U = Y_U$ for all $U \in \mathcal{F}(G)$. Let $\mathbf{z} = \mathbf{xy}$. For any cyclic G-set T,

$$z_T \equiv X_T Y_0^{\#T} + \psi_T \bmod pR,$$

where $\psi_T \in \mathbf{Z}[\{X_U, Y_U\}_{U<T}]$.

Here $\mathbf{x}$ is a "generic" Witt vector with first coordinate 0 and $\mathbf{y}$ is a "generic" Witt vector. A general element of $\mathfrak{m}$ and a general element of $\mathbf{W}_G(k)$ will be homomorphic images of them.

Proof. If $T = 0$ then $z_0 = X_0 Y_0$ so the result holds. Assume $T \neq 0$. Since $W_T \colon \mathbf{W}_G(R) \to R$ is multiplicative, $W_T(\mathbf{z}) = W_T(\mathbf{x}) W_T(\mathbf{y})$:

$$\sum_{U \leq T} \#U z_U^{\#T/\#U} = \left(\sum_{U \leq T} \#U x_U^{\#T/\#U}\right)\left(\sum_{U \leq T} \#U y_U^{\#T/\#U}\right). \tag{20}$$

Let $\#T = p^n$ with $n \geq 1$. Since T is a cyclic G-set, for each $i \leq n$ there is a unique $U_i \in \mathcal{F}(G)$ such that $U_i \leq T$ and $\#U_i = p^i$. Therefore (20) becomes

$$\sum_{i=0}^{n} \#U_i z_{U_i}^{p^{n-i}} = \left(\sum_{r=1}^{n} \#U_r X_{U_r}^{p^{n-r}}\right)\left(\sum_{s=0}^{n} \#U_s Y_{U_s}^{p^{n-s}}\right),$$

where the first sum on the right starts at $r = 1$ since $x_0 = 0$. Solving for $z_T = z_{U_n}$,

$$\begin{aligned} p^n z_T &= \left(\sum_{r=1}^{n-1} p^r X_{U_r}^{p^{n-r}} + p^n X_T\right)\left(Y_0^{p^n} + \sum_{s=1}^{n} p^s Y_{U_s}^{p^{n-s}}\right) - \sum_{i=0}^{n-1} p^i z_{U_i}^{p^{n-i}} \\ &= p^n X_T Y_0^{p^n} + p^n X_T \sum_{s=1}^{n} p^s Y_{U_s}^{p^{n-s}} + Y_0^{p^n} \sum_{r=1}^{n-1} p^r X_{U_r}^{p^{n-r}} \\ &\quad + \left(\sum_{r=1}^{n-1} p^r X_{U_r}^{p^{n-r}}\right)\left(\sum_{s=1}^{n} p^s Y_{U_s}^{p^{n-s}}\right) - \sum_{i=0}^{n-1} p^i z_{U_i}^{p^{n-i}}. \end{aligned}$$

In this last expression for $p^n z_T$, the second term is divisible by p^{n+1}, every part of the third term involves Y_0 and powers of X_U for $U < T$, the fourth term when expanded involves powers of X_U and Y_V for $U < T$ and $V < T$ except when $s = n$, whose terms are $\sum_{r=1}^{n-1} p^{r+n} X_{U_r}^{p^{n-r}} Y_T$ (a multiple of p^{n+1}), and the fifth term involves X_U and Y_V for $U < T$ and $V < T$ (each z_{U_i} for $i \leq n-1$ is a polynomial in X_U and Y_V where the indices U and V run over G-sets $\leq U_i < U_n = T$). Therefore if we reduce mod $p^{n+1}R$ we get

$$p^n z_T \equiv p^n X_T Y_0^{p^n} + \Psi_T(\{X_U, Y_U\}_{U<T}) \bmod p^{n+1}R$$

for some $\Psi_T \in \mathbf{Z}[\{X_U, Y_U\}_{U<T}]$. Since $z_T \in R$, every term except Ψ_T is in $p^n R$, so $\Psi_T \in p^n R$. Write $\Psi_T = p^n \psi_T$, with $\psi_T \in \mathbf{Z}[\{X_U, Y_U\}_{U<T}]$. Then

$$p^n z_T \equiv p^n X_T Y_0^{p^n} + p^n \psi_T \bmod p^{n+1} R \Longrightarrow z_T \equiv X_T Y_0^{p^n} + \psi_T \bmod pR.$$

For future reference,

$$\begin{aligned} \Psi_T(\{X_U, Y_U\}_{U<T}) &= Y_0^{\#T} \sum_{0<U<T} \#U X_U^{\#T/\#U} \\ &\quad + \sum_{0<U<T} \#U X_U^{\#T/\#U} \sum_{0<U<T} \#U Y_U^{\#T/\#U} \\ &\quad - \sum_{0<U<T} \#U z_U^{\#T/\#U} \end{aligned} \tag{21}$$

and $\psi_T = (1/\#T)\Psi_T$. □

For a finite collection $\{\mathbf{x}_1, \ldots, \mathbf{x}_r\} \subset \mathbf{W}_G(A)$, denote by $x_{i,T}$ the T-th coordinate of the vector $\mathbf{x}_i$.

Lemma 5.18. *For $r \geq 1$, let $R_r = \mathbf{Z}[\underline{X}_1, \ldots, \underline{X}_r, \underline{Y}_1, \ldots, \underline{Y}_r]$ be the polynomial ring in $2r$ sets of variables indexed by $\mathcal{F}(G)$, $\underline{X}_i = \{X_{i,U}\}_{1\leq i\leq r, U\in\mathcal{F}(G)}$ and $\underline{Y}_i = \{Y_{i,U}\}_{1\leq i\leq r, U\in\mathcal{F}(G)}$ indexed by $U \in \mathcal{F}(G)$. Let $\mathbf{x}_1, \ldots, \mathbf{x}_r$ and $\mathbf{y}_1, \ldots, \mathbf{y}_r$ be the Witt vectors in $\mathbf{W}_G(R_r)$ with coordinates $x_{i,0} = 0$, $x_{i,U} = X_{i,U}$ for $U \neq 0$ and $y_{i,U} = Y_{i,U}$ for all $U \in \mathcal{F}(G)$. Set $\mathbf{z} = \sum_{i=1}^{r} \mathbf{x}_i \mathbf{y}_i$. For any cyclic G-set T,*

$$z_T \equiv \sum_{i=1}^{r} X_{i,T} Y_{i,0}^{\#T} + f_T \bmod pR,$$

where $f_T \in \mathbf{Z}[\{X_{i,U}, Y_{i,U}\}_{U<T, 1\leq i\leq r}]$.

Proof. If $T = 0$ then $z_0 = \sum_{i=1}^r X_{i,0} Y_{i,0}$, so the result is true. Now let's assume $T \neq 0$. Set $\#T = p^n > 1$ and $\mathbf{z}_i = \mathbf{x}_i \mathbf{y}_i$, so $\mathbf{z} = \sum_{i=1}^r \mathbf{z}_i$. Since $W_T \colon \mathbf{W}_G(R_r) \to R_r$ is additive, $W_T(\mathbf{z}) = \sum_{i=1}^r W_T(\mathbf{z}_i)$:

$$\sum_{U\leq T} \#U z_U^{\#T/\#U} = \sum_{i=1}^{r} \sum_{U\leq T} \#U z_{i,U}^{\#T/\#U}.$$

Separating the terms for $U = T$ from $U < T$ and isolating z_T on one side,

$$p^n z_T = \sum_{i=1}^{r} p^n z_{i,T} + \sum_{i=1}^{r} \left(\sum_{U<T} \#U z_{i,U}^{\#T/\#U} \right) - \sum_{U<T} \#U z_U^{\#T/\#U}. \tag{22}$$

Each z_U is an integral polynomial in $X_{j,V}$ and $Y_{j,V}$ for $V \leq U$ and $j = 1, 2, \ldots, r$ and each $z_{i,U}$ is an integral polynomial in $X_{i,V}$ and $Y_{i,V}$ for $V \leq U$. Apply Lemma 5.17 to each $z_{i,T}$:

$$z_{i,T} \equiv X_{i,T}Y_{i,0}^{p^n} + \psi_{i,T} \bmod p\mathbf{Z}[\underline{X}_i, \underline{Y}_i], \tag{23}$$

where $\psi_{i,T} \in \mathbf{Z}[\{X_{i,U}, Y_{i,U}\}_{U<T}]$. Note $\psi_{i,T}$ depends only on variables indexed by G-sets strictly below T (see (21)). Substituting (23) into (22), and collecting terms,

$$p^n z_T \equiv p^n \sum_{i=1}^{r} X_{i,T}Y_{i,0}^{p^n} + F_T(\{X_{i,U}, Y_{i,U}\}_{U<T,1\leq i\leq r}) \bmod p^{n+1}R_r,$$

where F_T is an integral polynomial in the indicated variables. Since $z_T \in R_r$, we get $F_T \in p^n R_r$, so $F_T = p^n f_T$, where $f_T \in \mathbf{Z}[\{X_{i,U}, Y_{i,U}\}_{U<T,1\leq i\leq r}]$. Therefore

$$z_T \equiv \sum_{i=1}^{r} X_{i,T}Y_{i,0}^{p^n} + f_T \bmod pR_r.$$

□

Lemma 5.19. *For $r \geq 1$, let R_r be as in Lemma* 5.18 *and let $\mathbf{x}_1, \ldots, \mathbf{x}_r$ and $\mathbf{y}_1, \ldots, \mathbf{y}_r$ be defined in $\mathbf{W}_G(R)$ by $x_{i,0} = 0$, $x_{i,U} = X_{i,U}$ for $U \neq 0$, and $y_{i,U} = Y_{i,U}$ for all $U \in \mathcal{F}(G)$. Set $\mathbf{z} = \sum_{i=1}^{r} \mathbf{x}_i\mathbf{y}_i$. For $n \geq 1$ and a linked pair of cyclic G-sets T and T' such that $\#T = \#T' = p^n$,*

$$z_T - z_{T'} \equiv \sum_{i=1}^{r} (X_{i,T} - X_{i,T'})Y_{i,0}^{p^n} \bmod pR_r.$$

Proof. Set $\mathbf{z}_i = \mathbf{x}_i\mathbf{y}_i$, so $\mathbf{z} = \sum_{i=1}^{r} \mathbf{z}_i$. Since $W_T \colon \mathbf{W}_G(R_r) \to R_r$ is additive, $W_T(\mathbf{z}) = \sum_{i=1}^{r} W_T(\mathbf{z}_i)$:

$$\sum_{U\leq T} \#U z_U^{\#T/\#U} = \sum_{i=1}^{r} \sum_{U\leq T} \#U z_{i,U}^{\#T/\#U}. \tag{24}$$

Likewise with T' in place of T,

$$\sum_{U\leq T'} \#U z_U^{\#T'/\#U} = \sum_{i=1}^{r} \sum_{U\leq T'} \#U z_{i,U}^{\#T'/\#U}. \tag{25}$$

Since T and T' are linked, $\{U < T\} = \{U < T'\}$. Since we set $p^n = \#T = \#T'$, subtracting (25) from (24) gives us

$$p^n z_T - p^n z_{T'} = \sum_{i=1}^{r} (p^n z_{i,T} - p^n z_{i,T'}),$$

so

$$z_T - z_{T'} = \sum_{i=1}^{r}(z_{i,T} - z_{i,T'}). \tag{26}$$

Apply Lemma 5.17 to $z_{i,T}$ and $z_{i,T'}$ for $i = 1, \dots, r$:

$$z_{i,T} \equiv X_{i,T}Y_{i,0}^{p^n} + \psi_{i,T} \bmod p\mathbf{Z}[\underline{X}_i, \underline{Y}_i],\ z_{i,T'} \equiv X_{i,T'}Y_{i,0}^{p^n} + \psi_{i,T'} \bmod p\mathbf{Z}[\underline{X}_i, \underline{Y}_i] \tag{27}$$

where $\psi_{i,T}$ and $\psi_{i,T'}$ are $\mathbf{Z}$-polynomials in $X_{i,U}$ and $Y_{i,U}$ for $U < T$ and $u < T'$ respectively. By (21) and the fact that $\{U < T\} = \{U < T'\}$ (the key point!) we have $\psi_{i,T} = \psi_{i,T'}$. Substituting (27) into (26), the ψ's cancel and we're left with

$$z_T - z_{T'} \equiv \sum_{i=1}^{r}(X_{i,T} - X_{i,T'})Y_{i,0}^{p^n} \bmod pR_r.$$

□

Corollary 5.20. *For $r \geq 1$, pick $\mathbf{b}_1, \dots, \mathbf{b}_r \in \mathfrak{m}$ and $\mathbf{c}_1, \dots, \mathbf{c}_r \in \mathbf{W}_G(k)$. Set $\mathbf{a} = \sum_{i=1}^{r} \mathbf{b}_i\mathbf{c}_i$. For $n \geq 1$ and a pair of linked cyclic G-sets such that $\#T = \#T' = p^n$,*

$$a_T - a_{T'} = \sum_{i=1}^{r}(b_{i,T} - b_{i,T'})c_{i,0}^{p^n}.$$

Proof. Use Lemma 5.19 and functoriality. □

Remark 5.21. Lemmas 5.17, 5.18, 5.19 and Corollary 5.20 hold for any abelian pro-p G, not just $G = \mathbf{Z}_p^2$.

Just to recap, we are concerned with showing $\mathrm{Ann}_V = \mathrm{Ann}(\omega_V(1)) = \{\mathbf{w} \in \mathbf{W}_G(k) : \mathbf{w}\omega_V(1) = \mathbf{0}\}$ is not finitely generated, where $V \in \mathcal{F}(G)$ for $G = \mathbf{Z}_p^2$ with $\#V = p$, p odd, and k a field of characteristic p. Given a finite subset $\{\mathbf{b}_1, \dots, \mathbf{b}_r\}$ of $\mathfrak{m}$, using Corollary 5.20 we see that vectors in the ideal $(\mathbf{b}_1, \dots, \mathbf{b}_r)$ satisfy a relation among pairs of coordinates indexed by any linked cyclic G-sets T and T'. Since there are infinitely many such pairs of coordinates and only finitely many generators for the ideal, we will see that there are elements of Ann_V that can't appear in an ideal $(\mathbf{b}_1, \dots, \mathbf{b}_r)$.

Theorem 5.22. *Let p be an odd prime and $G = \mathbf{Z}_p^2$. For $V \in \mathcal{F}(G)$ such that $\#V = p$, the ideal Ann_V is not finitely generated.*

Proof. Pick $r \geq 1$ and $\mathbf{b}_1, \dots, \mathbf{b}_r \in \mathfrak{m}$. Let I be the ideal $(\mathbf{b}_1, \dots, \mathbf{b}_r)$. We want to show $I \neq \mathrm{Ann}_V$. In particular we will show $N_V \not\subset I$. For each $\mathbf{a} \in I$ there are $\mathbf{c}_1, \dots, \mathbf{c}_r \in \mathbf{W}_G(k)$ such that $\mathbf{a} = \sum_{i=1}^{r} \mathbf{b}_i\mathbf{c}_i$.

Recall the collection $\{T_j, T_j'\}$ for $j \geq 2$ such that T_j and T_j' are linked cyclic G-sets of size p^j. By Corollary 5.20,

$$a_{T_j} - a_{T_j'} = \sum_{i=1}^{r} (b_{i,T_j} - b_{i,T_j'}) c_{i,0}^{p^j}$$

for $j \geq 2$. For any $n \geq 2$, collect these equations for $j = 2, \ldots, n$ into a matrix equation over k: with $B_{i,j} = b_{i,T_j} - b_{i,T_j'}$,

$$\begin{bmatrix} a_{T_2} - a_{T_2'} \\ \vdots \\ a_{T_n} - a_{T_n'} \end{bmatrix} = \begin{bmatrix} B_{1,2} & \ldots & B_{r,2} & 0 & \ldots & 0 & \ldots & 0 \\ \vdots & & \vdots & & & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & B_{1,n} & \ldots & B_{r,n} \end{bmatrix} \begin{bmatrix} c_{1,0}^{p^2} \\ c_{2,0}^{p^2} \\ \vdots \\ c_{r,0}^{p^2} \\ c_{1,0}^{p^3} \\ c_{2,0}^{p^3} \\ \vdots \\ c_{r,0}^{p^3} \\ \vdots \\ c_{1,0}^{p^n} \\ c_{2,0}^{p^n} \\ \vdots \\ c_{r,0}^{p^n} \end{bmatrix}.$$

The matrix with entries $B_{i,j}$ only depends on coordinates of $\mathbf{b}_1, \ldots, \mathbf{b}_r$. For each $\mathbf{a} \in I = (\mathbf{b}_1, \ldots, \mathbf{b}_r)$, writing $\mathbf{a}$ as a $\mathbf{W}_G(k)$-linear combination of $\mathbf{b}_1, \ldots, \mathbf{b}_r$ shows there are $c_{1,0}, \ldots, c_{r,0}$ in k which solve the matrix equation above. If $I = \mathrm{Ann}_V$ then we can choose $\mathbf{a} \in N_V$. Then $a_{T_j} - a_{T_j'} = 2a_{T_j}$ since $a_{T_j} + a_{T_j'} = 0$. Hence $a_{T_j} - a_{T_j'}$ can be chosen arbitrarily in k for $j \geq 2$ since p is odd, so $2 \in k^\times$.

Thus the polynomial map $\varphi : k^r \to k^n$ given by

$$\begin{bmatrix} c_{1,0} \\ c_{2,0} \\ \vdots \\ c_{r,0} \end{bmatrix} \mapsto \begin{bmatrix} B_{2,1} & \dots & B_{2,r} & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & \dots & 0 & B_{3,1} & \dots & B_{3,r} & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & & & & & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & \dots & B_{n,1} & \dots & B_{n,r} \end{bmatrix} \begin{bmatrix} c_{1,0}^{p^2} \\ c_{2,0}^{p^2} \\ \vdots \\ c_{r,0}^{p^2} \\ c_{1,0}^{p^3} \\ c_{2,0}^{p^3} \\ \vdots \\ c_{r,0}^{p^3} \\ \vdots \\ c_{1,0}^{p^n} \\ c_{2,0}^{p^n} \\ \vdots \\ c_{r,0}^{p^n} \end{bmatrix}$$

would be surjective. If k is finite then $\#(k^r) \geq \#(k^n)$, so $r \geq n$. If k is infinite, by a transcendence degree argument $r \geq n$. We started with no connection between r and n, so by using $n > r$ we get a contradiction. □

Corollary 5.23. *The ring $\mathbf{W}_{\mathbf{Z}_p^2}(k)$ is not coherent when p is odd and k is a field of characteristic p.*

Proof. By Theorem 5.22, for $V \in \mathcal{F}(G)$ with $\#V = p$ the annihilator ideal of $\omega_V(1)$ is not finitely generated, so $\mathbf{W}_G(k)$ is not coherent. □

6 Zerodivisors of $\mathbf{W}_G(k)$

When k is a field of characteristic p, the classical Witt vectors $\mathbf{W}_{\mathbf{Z}_p}(k)$ form a domain. We will see this is not the case for the Witt vectors associated to any other nontrivial pro-p group G.

There is an isomorphism between $\mathbf{W}_G(\mathbf{Z})$ and the Burnside ring of almost finite G-sets. A G-set is almost finite when its orbits have finite size and the isomorphism type of any orbit appears finitely many times in G. One associates to $\mathbf{a} = (a_T)_{T \in \mathcal{F}(G)}$ in $\mathbf{W}_G(\mathbf{Z})$ the almost finite G-set $\coprod_T a_T T$, where T has multiplicity a_T (formal multiplicity if $a_T < 0$) [1]. In particular, T in the Burnside ring of G corresponds to $\omega_T(1)$ in $\mathbf{W}_G(\mathbf{Z})$.

Theorem 6.1. *If G is a nontrivial pro-p group and $G \not\cong \mathbf{Z}_p$, then $\mathbf{W}_G(\mathbf{F}_p)$ is not a domain, so $\mathbf{W}_G(A)$ is not a domain for any ring A of characteristic p.*

Proof. We treat separately the cases that G is pro-cyclic and not pro-cyclic.

The nontrivial pro-cyclic pro-p groups are (up to isomorphism) $\mathbf{Z}_p$ and $\mathbf{Z}/p^r\mathbf{Z}$ for some $r \geq 1$. When $G = \mathbf{Z}/p^r\mathbf{Z}$, $\mathbf{W}_G(\mathbf{F}_p) = \mathbf{Z}/p^{r+1}\mathbf{Z}$, so $\mathbf{W}_G(\mathbf{F}_p)$ isn't a domain for $r \geq 1$.

Assume from now on that G is not pro-cyclic. For any open normal subgroup N of G, we will show $\omega_{G/N}(1) - [G : N]$ is a zerodivisor of $\mathbf{W}_G(\mathbf{F}_p)$. When G acts diagonally on $G/N \times G/N$, each orbit is isomorphic to G/N, so the number of orbits is $[G : N]$. Viewing the Burnside ring of G as $\mathbf{W}_G(\mathbf{Z})$, this orbit decomposition of $G/N \times G/N$ turns into the equation $\omega_{G/N}(1)^2 = [G : N]\omega_{G/N}(1)$, so

$$\omega_{G/N}(1)(\omega_{G/N}(1) - [G : N]) = 0.$$

The homomorphism $\mathbf{W}_G(\mathbf{Z}) \to \mathbf{W}_G(\mathbf{F}_p)$ induced by reduction mod p from $\mathbf{Z}$ to $\mathbf{F}_p$ turns this equation into the same equation in $\mathbf{W}_G(\mathbf{F}_p)$, so

$$\omega_{G/N}(1)(\omega_{G/N}(1) - [G : N]) = 0 \text{ in } \mathbf{W}_G(\mathbf{F}_p).$$

The Witt vector $\omega_{G/N}(1)$ is not 0, so $\omega_{G/N}(1) - [G : N]$ is a zerodivisor of $\mathbf{W}_G(\mathbf{F}_p)$ for any open normal subgroup N of G.

It remains to show $\omega_{G/N}(1) - [G : N] \neq 0$ for some N. (This is impossible in the pro-cyclic case. If $G = \mathbf{Z}_p$ or $\mathbf{Z}/p^r\mathbf{Z}$ then there is only one open normal subgroup N of each index and for all of them $\omega_{G/N}(1) = [G : N]$ in $\mathbf{W}_G(\mathbf{F}_p)$.) We will focus on N of index p. In a finite p-group, all subgroups of index p are normal and in a noncyclic finite p-group there is more than one subgroup of index p, so G contains more than one open (normal) subgroup of index p. The G-sets G/N for different open subgroups N of index p are nonisomorphic, so there is more than one transitive G-set of size p up to isomorphism. Since $\omega_{G/N}(1) - p$ is a zerodivisor and p can't equal more than one $\omega_{G/N}(1)$ in $\mathbf{W}_G(\mathbf{F}_p)$, at least one $\omega_{G/N}(1) - p$ is a nonzero zerodivisor.

For the sake of completeness, we will show $p \neq \omega_{G/N}(1)$ for every open subgroup N of index p, so $\omega_{G/N}(1) - p$ and $\omega_{G/N}(1)$ are nontrivial zerodivisors. This will follow from a universal calculation for multiplication by p in Witt vectors over a polynomial ring, which will tell us p as a Witt vector in $\mathbf{W}_G(\mathbf{F}_p)$ is supported in more than one coordinate, while of course any $\omega_{G/N}(1)$ is supported only in the G/N-coordinate.

In $\mathbf{W}_G(\mathbf{Z}[\underline{X}])$, let $\mathbf{x}$ have T-coordinate X_T for all T and write

$$p\mathbf{x} = (f_T(\mathbf{x}))_{T \in \mathcal{F}(G)}$$

for some polynomials $f_T(\mathbf{x}) \in \mathbf{Z}[\underline{X}]$. Since $W_T \colon \mathbf{W}_G(\mathbf{Z}[\underline{X}]) \to \mathbf{Z}[\underline{X}]$ is additive, $pW_T(\mathbf{x}) = W_T((f_U(\mathbf{x}))_{U \in \mathcal{F}(G)})$, so

$$p \sum_{U \leq T} \varphi_T(U) X_U^{\#T/\#U} = \sum_{U \leq T} \varphi_T(U) f_U^{\#T/\#U}$$

for all T in $\mathcal{F}(G)$. Taking $T = 0$, we get $f_0 = pX_0$. Taking $\#T = p$,

$$p(X_0^p + \varphi_T(T)X_T) = f_0^p + \varphi_T(T)f_T = p^pX_0^p + \varphi_T(T)f_T.$$

Since $T \cong G/N$ where N is normal, $\varphi_T(T) = \#T = p$. Therefore

$$f_T = (1 - p^{p-1})X_0^p + pX_T.$$

By functoriality, when A is a commutative ring of characteristic p and $\mathbf{a} \in \mathbf{W}_G(A)$, $p\mathbf{a}$ has 0-coordinate $f_0(\mathbf{a}) = pa_0 = 0$ and for $\#T = p$ the T-coordinate of $p\mathbf{a}$ is $f_T(\mathbf{a}) = a_0^p$. In particular, $p = p \cdot (1, 0, 0, \dots)$ has T-coordinate 1 when $\#T = p$ and there is more than one such T when G is not pro-cyclic. So $p \neq \omega_{G/N}(1)$ in $\mathbf{W}_G(A)$ for any N of index p. □

Remark 6.2. It is not hard to see when $G = \mathbf{Z}_p^2$ each p^r for $r > 0$ is supported in $\mathbf{W}_G(\mathbf{F}_p)$ on more than one coordinate. This implies $\omega_{G/H}(1) - [G : H]$ is a nonzero zerodivisor in $\mathbf{W}_{\mathbf{Z}_p^2}(\mathbf{F}_p)$ for any nontrivial open subgroup H of $\mathbf{Z}_p^2$.

Although $\mathbf{W}_G(k)$ is not a domain and is not Noetherian, this is not a pathological state of affairs among p-adic rings. For instance, the ring $C(\mathbf{Z}_p, \mathbf{Q}_p)$ of continuous functions from $\mathbf{Z}_p$ to $\mathbf{Q}_p$ is not a domain and is not Noetherian. This ring is reduced. So we ask: is $\mathbf{W}_G(k)$ reduced? In the case $G = \mathbf{Z}_p^2$ for any p we will show it is and we will show in some other cases it is not.

To prove that $\mathbf{W}_{\mathbf{Z}_p^2}(k)$ is reduced when k has characteristic p, we seek the right coordinate to look at in a power of a nonzero Witt vector to know that the power is also not $\mathbf{0}$.

Say $\mathbf{x} \in \mathbf{W}_G(k)$ and $\mathbf{x} \neq \mathbf{0}$. It is natural to consider how $\mathbf{x}$ sits in the descending ideal filtration $\{I_{p^n}\}$: there is some I_{p^n} for which $\mathbf{x} \in I_{p^n}$ and n is as large as possible, so $x_T = 0$ for $\#T < p^n$ and some x_T is nonzero where $\#T = p^n$. Then $\mathbf{x}^2 \in I_{p^{2n}}$ (Corollary 3.19), and we can anticipate (if $\mathbf{W}_G(k)$ is reduced) that $\mathbf{x}^2$ has a nonzero coordinate at some G-set of size p^{2n}. Which one? We need a way to predict a nonzero coordinate in $\mathbf{x}^2$ when $\mathbf{x} \neq \mathbf{0}$.

To do this we will again utilize the concept of level. Recall for $G = \mathbf{Z}_p^d$ that the *level* of $T \in \mathcal{F}(G)$ is the largest $n \geq 0$ such that $T \geq G/p^nG$. The level function $\mathrm{Lev}\colon \mathcal{F}(G) \to \mathbf{N}$ respects the partial orderings on both sets:

Lemma 6.3. *Let $G = \mathbf{Z}_p^d$. If $U \leq T$ in $\mathcal{F}(G)$ then* $\mathrm{Lev}(U) \leq \mathrm{Lev}(T)$.

Proof. Let $n = \mathrm{Lev}(U)$, so $U \geq G/p^nG$. Since $T \geq U$, we have $T \geq G/p^nG$, so $\mathrm{Lev}(T) \geq n$. □

Note that if $U < T$ and $d \geq 2$ it need not follow that $\mathrm{Lev}(U) < \mathrm{Lev}(T)$: we might have $\mathrm{Lev}(U) = \mathrm{Lev}(T)$. For example, if $U = G/H$ and $T = G/K$ where $H = p\mathbf{Z}_p^d = p\mathbf{Z}_p^{d-1} \times p\mathbf{Z}_p$ and $K = p\mathbf{Z}_p^{d-1} \times p^2\mathbf{Z}_p$ then $K \subset H$ so $U < T$ and $\mathrm{Lev}(U) = \mathrm{Lev}(T) = 1$.

Lemma 6.4. *Let $G = \mathbf{Z}_p^d$ and $T \in \mathcal{F}(G)$ have level n. Write $T \cong G/H$ with $H \subset p^n\mathbf{Z}_p^d$ and $H \not\subset p^{n+1}\mathbf{Z}_p^d$ so $H = p^n\widehat{H}$ for a unique open subgroup $\widehat{H}$ of $\mathbf{Z}_p^d$. Set $\widehat{T} = G/\widehat{H}$. Then $\widehat{T}$ has level 0. Moreover, if $U \in \mathcal{F}(G)$ and $\mathrm{Lev}(U) = n$ then $U \leq T$ if and only if $\widehat{U} \leq \widehat{T}$.*

Proof. By choosing a suitable basis of $\mathbf{Z}_p^d$, we may assume $H = p^{a_1}\mathbf{Z}_p \times \ldots \times p^{a_d}\mathbf{Z}_p$. The statement that T has level n means $n = \min\{a_1, \ldots, a_d\}$, so $H = p^n(p^{b_1}\mathbf{Z}_p \times \ldots \times p^{b_d}\mathbf{Z}_p)$ with some $b_i = 0$. Then $\widehat{H} = p^{b_1}\mathbf{Z}_p \times \ldots \times p^{b_d}\mathbf{Z}_p$ and $\widehat{T}$ has level 0.

To prove the second claim, write $U \cong G/K$ and $K = p^n\widehat{K}$. We have $U \leq T$ if and only if $H \subset K$ and $\widehat{U} \leq \widehat{T}$ if and only if $\widehat{H} \subset \widehat{K}$. The conditions $H \subset K$ and $\widehat{H} \subset \widehat{K}$ are the same. □

Lemma 6.5. *For $G = \mathbf{Z}_p^d$ with $d \geq 2$ and $T \in \mathcal{F}(G)$, set $\#T = p^n$. For each $m \geq n$, there exist T' such that $\#T' = p^m$, $T \leq T'$ and $\mathrm{Lev}(T) = \mathrm{Lev}(T')$.*

Proof. Write $T = G/H$. Choose a $\mathbf{Z}_p$-basis $\{e_1, e_2, \ldots, e_d\}$ of $\mathbf{Z}_p^d$ such that $H = \sum_{i=1}^d \mathbf{Z}_p p^{a_i} e_i$. Without loss of generality, assume $a_1 \leq a_2 \leq \ldots \leq a_d$ and set $K = \sum_{i=1}^{d-1} \mathbf{Z}_p p^{a_i} e_i + \mathbf{Z}_p p^{a_d+m-n} e_d$. Then $K \subset H$ and $[H : K] = p^{m-n}$ so G/K is a cover of G/H. Since $a_1 \leq a_2 \leq \ldots \leq a_d$ and $d \geq 2$, $\min\{a_1, a_2, \ldots, a_d\} = \min\{a_1, a_2, \ldots, a_d + m - n\}$, so $\mathrm{Lev}(G/K) = \mathrm{Lev}(G/H)$. □

Consider Figure 3. The two horizontal lines divide the diagram into regions of $\mathbf{Z}_2^2$-sets with the same level. Lemma 6.5 just says that these levels go infinitely far out in the frame.

Returning to the assumption $G = \mathbf{Z}_p^2$ we have the following lemma.

Lemma 6.6. *When $G = \mathbf{Z}_p^2$ and T and T' in $\mathcal{F}(G)$ satisfy $T \leq T'$ and $\mathrm{Lev}(T) = \mathrm{Lev}(T')$,*

$$\{U \in \mathcal{F}(G) : U \leq T' \text{ and } \mathrm{Lev}(U) = \mathrm{Lev}(T) \text{ and } \#U = \#T\} = \{T\}.$$

Proof. We have already noted that the set of G-sets of level zero is a tree, so the property is obviously true when $\mathrm{Lev}(T) = \mathrm{Lev}(T') = 0$. Using Lemma 6.4 one has the result for any level. □

Lemma 6.7. *Let $G = \mathbf{Z}_p^2$, A be a nonzero commutative ring, and choose any nonzero $\mathbf{a} \in W_G(A)$. There is a $T_0 \in \mathcal{F}(G)$ such that $a_{T_0} \neq 0$ and $a_U = 0$ under either of the following conditions:*

- $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$,
- $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ *and* $\#U < \#T_0$,

Proof. Given $\mathbf{a} \neq \mathbf{0}$ in $\mathbf{W}_G(A)$, among $\{T : a_T \neq 0\}$ first select all T with minimal level, and then among the T of that minimal level, choose one T of minimal size. Call that T_0.

If $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$ then $a_U = 0$ since T_0 is a nonzero coordinate with minimal level. If $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ and $\#U < \#T_0$ then $a_U = 0$ since otherwise T_0 is not a nonzero coordinate of minimal size among nonzero coordinates of minimal level. □

Remark 6.8. Lemma 6.7 is expressed in a form convenient for the applications we have in mind, but it's not a result about nonzero Witt vectors so much as a property of $\mathcal{F}(G)$: for any nonempty subset $\mathcal{S}$ of $\mathcal{F}(G)$, there is a $T_0 \in \mathcal{S}$ such that $U \notin \mathcal{S}$ if $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$, or if $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ and $\#U < \#T_0$.

Remark 6.9. In our application of Lemma 6.7 it is important to note the order in which the concepts are minimized. Here we are first choosing nonzero G-sets of minimal level, then among those we choose one of minimal size. These two minimizations do not commute. Figure 5 depicts a nonzero element of $\mathbf{W}_{\mathbf{Z}_2^2}(k)$. The T coordinate is the one of minimal size first and then level, whereas the U coordinate is the one of minimal level first and then size.

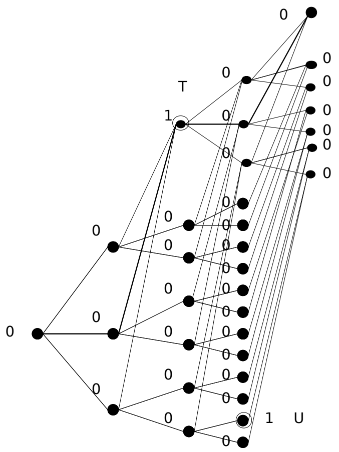

Figure 5: Nonzero element in $\mathbf{W}_G(\mathbf{F}_2)$, $G = \mathbf{Z}_2^2$.

Now we will use the concept of level to prove something about multiplication in $\mathbf{W}_G(k)$. The end of the next lemma identifies a formula for a specific coordinate in the product of two Witt vectors if all the "smaller" coordinates are 0. It is analogous to something simple when $G = \mathbf{Z}_p$: if $\mathbf{a} = p^n(a_0 + p\mathbf{a}')$ and $\mathbf{b} = p^n(b_0 + p\mathbf{b}')$ then $\mathbf{ab} = p^{2n}(a_0b_0 + p\mathbf{c})$. (It is not assumed that a_0 and b_0 are nonzero.) There is a similar formula even if the p-powers in $\mathbf{a}$ and $\mathbf{b}$ are not equal, but for $G = \mathbf{Z}_p^d$ with $d \geq 2$ we don't have a formula that broad. It seems to be the price we pay for $\mathbf{W}_G(k)$ not being a domain.

Lemma 6.10. *For $G = \mathbf{Z}_p^2$, let $\mathbf{a}$ and $\mathbf{b}$ be in $\mathbf{W}_G(k)$ such that there is a $T_0 \in \mathcal{F}(G)$ such that $a_U = b_U = 0$ if $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$, or if $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ and $\#U < \#T_0$. Set $\#T_0 = p^n$. For any $T \in \mathcal{F}(G)$ with size p^{2n} such that $T_0 \leq T$ and $\mathrm{Lev}(T_0) = \mathrm{Lev}(T)$, the product $\mathbf{ab}$ has T-coordinate $(a_{T_0}b_{T_0})^{p^n}$.*

Proof. Let $R = \mathbf{Z}[\underline{X}, \underline{Y}]$. Define $\mathbf{x}, \mathbf{y}$ in $\mathbf{W}_G(R)$ by

$$x_U = \begin{cases} 0 & \text{if } \operatorname{Lev}(U) < \operatorname{Lev}(T_0), \\ 0 & \text{if } \operatorname{Lev}(U) = \operatorname{Lev}(T_0) \text{ and } \#U < p^n, \\ X_U & \text{otherwise,} \end{cases}$$

and

$$y_U = \begin{cases} 0 & \text{if } \operatorname{Lev}(U) < \operatorname{Lev}(T_0), \\ 0 & \text{if } \operatorname{Lev}(U) = \operatorname{Lev}(T_0) \text{ and } \#U < p^n, \\ Y_U & \text{otherwise.} \end{cases}$$

and set $\mathbf{z} = \mathbf{xy}$. For any G-set T of size p^{2n} with $T_0 \leq T$ and $\operatorname{Lev}(T_0) = \operatorname{Lev}(T)$ we will show $z_T \equiv (X_{T_0} Y_{T_0})^{p^n} \bmod pR$. By functoriality the lemma would then follow.

For any G-set T, $W_T(\mathbf{z}) = W_T(\mathbf{x}) W_T(\mathbf{y})$:

$$\sum_{U \leq T} \#U z_U^{\#T/\#U} = \left(\sum_{U \leq T} \#U x_U^{\#T/\#U} \right) \left(\sum_{U \leq T} \#U y_U^{\#T/\#U} \right). \tag{28}$$

By Lemma 6.5 we can choose $T \geq T_0$ such that $\#T = p^{2n}$ and $\operatorname{Lev}(T) = \operatorname{Lev}(T_0)$. First we look at the left side of (28). Let $V < T$, so $\#V < p^{2n}$. By Lemma 6.3 $\operatorname{Lev}(V) \leq \operatorname{Lev}(T) = \operatorname{Lev}(T_0)$. So either $\operatorname{Lev}(V) < \operatorname{Lev}(T)$ or $\operatorname{Lev}(V) = \operatorname{Lev}(T)$. For all $U < V$ with $\#U < p^n$, both x_U and y_U are zero by hypothesis. The proof of Lemma 3.15 tells us that $z_V \equiv 0 \bmod pR$ when $V < T$ and $\#V < p^{2n}$. So $\#V z_V^{\#T/\#V} \equiv 0 \bmod p^{2n+1}R$ for $V < T$ and $\#V < p^{2n}$, so the left side of (28) is $p^{2n} z_T \bmod p^{2n+1}R$.

Now we turn to the right side of (28). If $U \leq T$ then $\operatorname{Lev}(U) \leq \operatorname{Lev}(T)$ (Lemma 6.3) and since $\operatorname{Lev}(T) = \operatorname{Lev}(T_0)$ our hypotheses tells us $x_U = 0$ and $y_U = 0$ if $\operatorname{Lev}(U) < \operatorname{Lev}(T)$, or if $\operatorname{Lev}(U) = \operatorname{Lev}(T)$ and $\#U < p^n$. So the only U-terms in each sum on the right side of (28) that are not automatically 0 have $\operatorname{Lev}(U) = \operatorname{Lev}(T)$ and $\#U \geq p^n$.

Dropping the terms in (28) where $x_U = 0$ and $y_U = 0$ and reducing modulo $p^{2n+1}R$,

$$p^{2n} z_T \equiv \left(\sum_{\substack{U \leq T \\ \operatorname{Lev}(U) = \operatorname{Lev}(T) \\ \#U \geq p^n}} \#U X_U^{\#T/\#U} \right) \left(\sum_{\substack{U \leq T \\ \operatorname{Lev}(U) = \operatorname{Lev}(T) \\ \#U \geq p^n}} \#U Y_U^{\#T/\#U} \right) \bmod p^{2n+1}R.$$

Each summand in the two sums has a coefficient divisible at least by p^n, so any product of a term from each sum is divisible by p^{2n}. A term divisible by p^{n+1} in one sum has a product with any term in the other sum that is 0 mod $p^{2n+1}R$, so

$$p^{2n}z_T \equiv \left(\sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U=p^n}} p^n X_U^{p^n} \right) \left(\sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U=p^n}} p^n Y_U^{p^n} \right) \bmod p^{2n+1}R.$$

Dividing through by p^{2n} and using additivity of the pth power map in R/pR,

$$z_T \equiv \left(\sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U=p^n}} X_U \cdot \sum_{\substack{U \leq T \\ \mathrm{Lev}(U)=\mathrm{Lev}(T) \\ \#U=p^n}} Y_U \right)^{p^n} \bmod pR. \tag{29}$$

What are the U lying below T in $\mathcal{F}(G)$ with the same level as T and of size p^n? One example is $U = T_0$. By Lemma 6.6 this is the only example, so $z_T \equiv (X_{T_0}Y_{T_0})^{p^n} \bmod pR$. □

We will only apply Lemma 6.10 when the two Witt vectors are equal, i.e., to the square of a nonzero element of $\mathbf{W}_G(k)$.

Remark 6.11. Most of the proof of Lemma 6.10 goes through for $G = \mathbf{Z}_p^d$ for $d \geq 3$ and not just $d = 2$. In fact (29) is true for $G = \mathbf{Z}_p^d$ for $d \geq 2$ and it was only at the last step where we used the fact that $d = 2$, which hinged on Lemma 6.6. Lemma 6.6 is not true for $G = \mathbf{Z}_p^d$ with $d \geq 3$ since the level 0 part of $\mathcal{F}(\mathbf{Z}_p^d)$ is not a tree. For example when $d \geq 3$, $\mathbf{Z}_p^d/(\mathbf{Z}_p \times p\mathbf{Z}_p \times p^a\mathbf{Z}_p^{p-2})$ with $a \geq 1$ is not a cyclic group and so its strict downset is not a chain.

Theorem 6.12. *For any field k of characteristic p, the ring $\mathbf{W}_G(k)$ is reduced for $G = \mathbf{Z}_p^2$.*

Proof. Let $\mathbf{v}$ be nonzero in $\mathbf{W}_G(k)$. If $v_0 \neq 0$ then $\mathbf{v} \in \mathbf{W}_G(k)^\times$ by Theorem 3.20. Otherwise $\mathbf{v} \in \mathfrak{m}$ and it suffices to show for all $n \in \mathbf{Z}^+$ that $\mathbf{v}^{2^n}$ is nonzero. Thus it suffices to show if $\mathbf{v} \in \mathfrak{m}$ and $\mathbf{v} \neq \mathbf{0}$ then $\mathbf{v}^2 \neq \mathbf{0}$. By Lemma 6.7 there is a $T_0 \in \mathcal{F}(G)$ such that v_{T_0} is nonzero but v_U is zero for all $U \in \mathcal{F}(G)$ where $\mathrm{Lev}(U) < \mathrm{Lev}(T_0)$ or where $\mathrm{Lev}(U) = \mathrm{Lev}(T_0)$ and $\#U < \#T_0$. Lemma 6.10 with $\mathbf{a} = \mathbf{b} = \mathbf{v}$ tells us that $\mathbf{v}^2$ has a coordinate equal to $v_{T_0}^{2\#T_0} \neq 0$, so $\mathbf{v}^2 \neq \mathbf{0}$. □

Since $\mathbf{W}_{\mathbf{Z}_p^2}(k)$ is reduced, the intersection of all prime ideals is $\{\mathbf{0}\}$. So we have an embedding $\mathbf{W}_{\mathbf{Z}_p^2}(k) \hookrightarrow \prod_{\mathfrak{p}} \mathbf{W}_{\mathbf{Z}_p^2}(k)/\mathfrak{p}$ by reduction mod $\mathfrak{p}$ for all prime ideals $\mathfrak{p}$. The latter ring is a product of domains. A natural question to ask is: what are the rings $\mathbf{W}_{\mathbf{Z}_p^2}(k)/\mathfrak{p}$? For $G = \mathbf{Z}_p^d$ we can describe a natural collection of prime ideals in $\mathbf{W}_G(k)$. Let $f\colon \mathbf{Z}_p^d \twoheadrightarrow \mathbf{Z}_p$ be a continuous surjective group homomorphism. So f induces a surjective ring homomorphism $\mathbf{W}_{\mathbf{Z}_p^d}(k) \twoheadrightarrow \mathbf{W}_{\mathbf{Z}_p}(k)$ whose kernel is a prime ideal. We want to make this ring homomorphism explicit in terms of the frame of $\mathbf{Z}_p^d$, so we can visualize all these prime ideals.

Pick a $\mathbf{Z}_p$-basis $\{e_1,\dots,e_d\}$ of $\mathbf{Z}_p^d$ so that $\mathbf{Z}_p^d = \sum_{i=1}^d \mathbf{Z}_p e_i$ and for some $d' \leq d$, $\ker f = \sum_{i=1}^{d'} \mathbf{Z}_p p^{a_i} e_i$ where $a_0,\dots,a_{d'} \geq 0$. Then $\mathbf{Z}_p^d/\ker f = \sum_{i=1}^{d'}(\mathbf{Z}_p/p^{a_i}\mathbf{Z}_p)\overline{e_i} + \sum_{i=d'+1}^{d}\mathbf{Z}_p\overline{e_i}$. Since we know this quotient is isomorphic to $\mathbf{Z}_p$, $d' = d-1$ and $a_1,\dots,a_{d-1} = 0$, so $f(x_1e_1+\ldots+x_de_d) = f(e_d)x_d$ where $f(e_d) \in \mathbf{Z}_p^\times$. After readjusting our basis, we can assume $f(e_d) = 1$ so f is projection onto the e_d-coordinate. Set $N = \ker f$. The open subgroups of $\mathbf{Z}_p^d$ containing N are $N + \mathbf{Z}_p p^r e_d$ for $r \geq 0$, so the image of $\mathcal{F}(\mathbf{Z}_p^d/N)$ in $\mathcal{F}(\mathbf{Z}_p^d)$ is the $\mathbf{Z}_p^d$-sets

$$\mathbf{Z}_p^d/(N+\mathbf{Z}_p p^r e_d) = \sum_{i=1}^{d}\mathbf{Z}_p e_i/(\sum_{i=1}^{d-1}\mathbf{Z}_p e_i + \mathbf{Z}_p p^r e_d), \tag{30}$$

which form a chain of cyclic $\mathbf{Z}_p^d$-sets of level 0, like all cyclic $\mathbf{Z}_p^d$-sets.

When $d = 2$, all $\mathbf{Z}_p^2$-sets of level 0 are cyclic and the sets of level 0 are a tree, so (30) as r varies is a path in level 0 in $\mathcal{F}(\mathbf{Z}_p^2)$. See Figure 6.

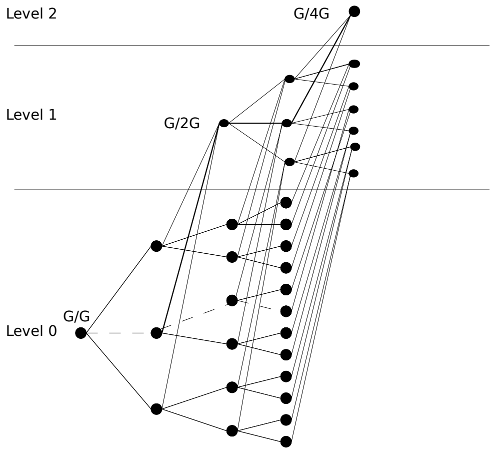

Figure 6: Level 0 path in $\mathcal{F}(G)$, $G = \mathbf{Z}_2^2$.

The ring homomorphism $\mathbf{W}_{\mathbf{Z}_p^d}(k) \twoheadrightarrow \mathbf{W}_{\mathbf{Z}_p}(k)$ induced by f is projection onto the coordinates indexed by (30), so the kernel of this ring homomorphism is a height one prime ideal in $\mathbf{W}_{\mathbf{Z}_p^d}(k)$. Denote it by $\mathfrak{p}_f$. All cyclic $\mathbf{Z}_p^d$-sets have the form $\sum_{i=1}^{d-1}\mathbf{Z}_p e_i + \mathbf{Z}_p p^r e_d$ for some $\mathbf{Z}_p$-basis $\{e_1,\dots,e_d\}$ and $r \geq 0$, so

$$\bigcap_{f:\mathbf{Z}_p^d \twoheadrightarrow \mathbf{Z}_p} \mathfrak{p}_f \cap \mathfrak{m} = \bigcap_{f:\mathbf{Z}_p^d \twoheadrightarrow \mathbf{Z}_p} \mathfrak{p}_f = \{\mathbf{a} \in \mathbf{W}_{\mathbf{Z}_p^d}(k) \colon a_T = 0 \text{ if } T \text{ is cyclic}\},$$

which is not $\{\mathbf{0}\}$ since cyclic $\mathbf{Z}_p^d$-sets have level 0. Theorem 6.12 tells us the nilradical of $\mathbf{W}_{\mathbf{Z}_p^2}(k)$ is $\{\mathbf{0}\}$. Therefore there must be additional non-maximal prime ideals in $\mathbf{W}_{\mathbf{Z}_p^2}(k)$ beyond those we have constructed here (and similarly in $\mathbf{W}_{\mathbf{Z}_p^d}(k)$ for $d \geq 3$ if we could show all these rings are reduced). Further examples of prime ideals in $\mathbf{W}_{\mathbf{Z}_p^2}(k)$ have not yet been found.

Next we will see that $\mathbf{W}_G(k)$ is not reduced for $G = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}_p$ where p is odd and k a field of characteristic p. Viewing G as $\mathbf{Z}_p^2/(p\mathbf{Z}_p \times \{0\})$ the frame of this group consists of $\mathbf{Z}_p^2/H$ where $p\mathbf{Z}_p \times \{0\} \subset H \subset \mathbf{Z}_p^2$. Since $H \not\subset p^2\mathbf{Z}_p^2$, $\mathcal{F}(\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}_p)$ only involves part of the frame $\mathcal{F}(\mathbf{Z}_p^2)$ that has level zero and one. In particular, the subgroups H arise from taking a particular path in the level one portion of the frame of $\mathbf{Z}_p^2$, $T_1 \leq T_2 \leq T_3 \ldots$ where $T_n = \mathbf{Z}_p^2/(p\mathbf{Z}_p \times p^n\mathbf{Z}_p)$ and all G-sets lying below the T_i. See Figure 7.

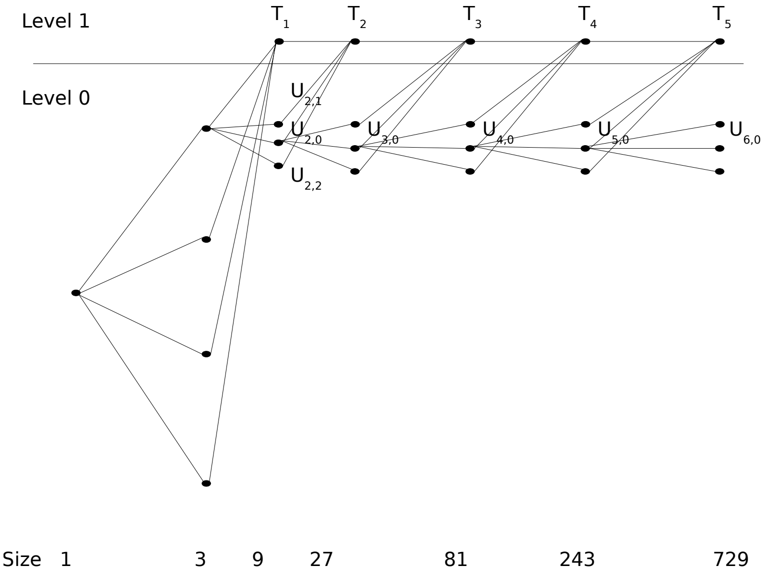

Figure 7: Portion of the frame $\mathcal{F}(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}_3)$.

Theorem 6.13. *If $G = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}_p$ and p is odd, then $\mathbf{W}_G(\mathbf{F}_p)$ is not reduced.*

Proof. Let's first establish some notation. Recall that $\omega_T(a)$ is the Witt vector which is zero at all coordinates except the coordinate T where it has the value a. We can think of $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}_p$ as $\mathbf{Z}_p^2/N$ where $N = p\mathbf{Z} \times \{0\}$. Doing so gives us an order-preserving correspondence between all G/N-sets and the G-sets of the form G/H where $N \subset H$. Fix a $\mathbf{Z}_p$-basis $\{e_1, e_2\}$ of $\mathbf{Z}_p^2$ so that $N = \mathbf{Z}_p(pe_1) \oplus \{0\}$. Denote by $\{T_1, T_2, \ldots\}$ the $\mathbf{Z}_p^2$-sets where the stabilizer of T_i is $\mathbf{Z}_p(pe_1) \oplus \mathbf{Z}_p(p^ie_2)$, so $T_i \leq T_{i+1}$. For $i \geq 2$, T_i covers exactly $p+1$ G-sets: T_{i-1} and p others $U_{i,0}$, $U_{i,1}$,...,$U_{i,p-1}$ where the stabilizer of $U_{i,0}$ is $\mathbf{Z}_pe_1 \oplus \mathbf{Z}_p(p^ie_2)$ for $i \geq 2$ and the stabilizer of $U_{i,j}$ for $j = 1, \ldots, p-1$ is $\mathbf{Z}_p(pe_1 + je_2) + \mathbf{Z}_p(p^{i-1}e_2)$. It is easy to verify for $i \geq 2$ that $U_{i,0}$ is covered by $T_i, U_{i+1,0}, \ldots, U_{i+1,p-1}$. See the labeling in Figure 7. So,

- the unique cover of T_i is T_{i+1},
- the unique cover of $U_{i,j}$ is T_i for $0 < j < p$, and
- the covers of $U_{i,0}$ are T_i and $U_{i+1,j}$ for $0 \le j < p$.

Since $\mathcal{F}(G) = \mathcal{F}(\mathbf{Z}_p^2/N)$ embeds in $\mathcal{F}(\mathbf{Z}_p^2)$ we will think of the elements in the image, $\{T_i\}_{i\ge 1}$ and $\{U_{i,j}\}_{i\ge 2, j=0,\ldots,p-1}$, as elements of $\mathcal{F}(G)$.

The following mod p congruence in $\mathbf{W}_G(\mathbf{Z})$ will complete the proof that $\mathbf{W}_G(\mathbf{F}_p)$ is not reduced. In $\mathbf{W}_G(\mathbf{Z})$ define $\mathbf{x} = \omega_{U_{2,1}}(1)+\omega_{U_{2,2}}(-1)$ and $\mathbf{m} = \mathbf{x}^2$. We will show $m_T \equiv 0 \bmod p\mathbf{Z}[\{X_U\}_{U\in\mathcal{F}(G)}]$ for all T, so under the natural ring homomorphism $\mathbf{W}_G(\mathbf{Z}) \to \mathbf{W}_G(\mathbf{F}_p)$, $\mathbf{x}$ has a nonzero image whose square is $\mathbf{0}$.

We aim first to show

$$W_T(\mathbf{x}) = \begin{cases} p^2 & \text{if } T = U_{2,1}, \\ -p^2 & \text{if } T = U_{2,2}, \\ 0 & \text{otherwise.} \end{cases}$$

If $\#T < p^2$, then $W_T(\mathbf{x}) = 0$. Also $W_{T_1}(\mathbf{x}) = 0$. Since $x_T = 0$ for $\#T = p$ and $x_{U_{i,0}} = 0$ for all i, $W_{U_{i,j}}(\mathbf{x}) = 0$ for all $i > 2$ and $j = 0, \ldots, p-1$ and $W_{U_{2,1}}(\mathbf{x}) = p^2$ and $W_{U_{2,2}}(\mathbf{x}) = -p^2$. We now check that $W_{T_i}(\mathbf{x}) = 0$ for all $i > 1$. We do this by direct verification. By definition $W_{T_i}(\mathbf{x}) = \sum\limits_{U\le T_i} \#U x_U^{\#T_i/\#U}$. The only nonzero coordinates in $\mathbf{x}$ lying below T_i are $U_{2,1}$ and $U_{2,2}$. Noting that $\#U_{2,j} = p^2$ for each $j = 0, \ldots, p-1$ and removing the zero terms in the sum we have $W_{T_i}(\mathbf{x}) = p^2(1)^{\#T_i/p^2} + p^2(-1)^{\#T_i/p^2} = p^2(1-1) = 0$ since p is odd.

We now turn our attention to the Witt vector $\mathbf{m} = \mathbf{x}^2$. For any G-set $T \notin \{U_{2,1}, U_{2,2}, T_i : i \ge 2\}$, $W_U(\mathbf{x}) = 0$ for all $U \le T$, so $W_U(\mathbf{m}) = 0$ for all $U \le T$, which by induction gives that $m_T = 0$ for any G-set $T \ne U_{2,1}, U_{2,2}$ or T_i for $i \ge 2$. We will show that $m_T \equiv 0 \bmod p\mathbf{Z}[\{X_U\}_{U\in\mathcal{F}(G)}]$ for any $T \in \{U_{2,1}, U_{2,2}, T_i \colon i \ge 2\}$.

We start with $U_{2,1}$. By definition $W_{U_{2,1}}(\mathbf{m}) = W_{U_{2,1}}(\mathbf{x}^2) = W_{U_{2,1}}(\mathbf{x})^2 = p^4$. Expanding this out we have

$$\sum_{V\le U_{2,1}} \#V m_V^{\#U_{2,1}/\#V} = p^4. \tag{31}$$

Since $m_V = 0$ for $V < U_{2,1}$ the only nonzero term on the left hand side of (31) is $p^2 m_{U_{2,1}}$ and so $p^2 m_{U_{2,1}} = p^4$, which gives $m_{U_{2,1}} \equiv 0 \bmod p$ (in fact this congruence is true mod p^2 but we only need it mod p). A similar calculation shows that $m_{U_{2,2}} \equiv 0 \bmod p$ as well.

Consider the coordinate T_i for $i \ge 2$. We have already shown $W_{T_i}(\mathbf{m}) = W_{T_i}(\mathbf{x})^2 = 0$. Expanding this out we have

$$\sum_{V\le T_i} \#V m_V^{\#T_i/\#V} = 0. \tag{32}$$

The only nonzero terms in (32) are those with $V = U_{2,1}$ and $V = U_{2,2}$ and $V = T_j$ for $j = 1, \ldots, i$. Removing the zero terms, (32) becomes $p^2 m_{U_{2,1}}^{\#T_i/p^2} + p^2 m_{U_{2,2}}^{\#T_i/p^2} + \#T_i m_{T_i} = 0$. Since $\#T_i = p^{i+1}$, moving terms over we see that $p^{i+1} m_{T_i} = -p^2(m_{U_{2,1}}^{p^{i-1}} + m_{U_{2,2}}^{p^{i-1}}) = -2p^2(p^{2p^{i-1}})$, so $m_{T_i} = -2p^{2p^{i-1}-(i-1)}$. We note that $2p^{i-1} > i-1$ for $i \geq 2$, which shows $m_{T_i} \equiv 0 \bmod p$. □

Acknowledgments

This paper is based on the author's Ph.D. thesis at the University of Connecticut [6]. The author is forever indebted to his advisor Keith Conrad without whose endless patience and support this work would not have been possible. The author would also like to thank Sarah Glaz, Álvaro Lozano-Robledo, and Jeremy Teitelbaum for many helpful and enlightening discussions and editorial suggestions and to Jesse Elliott, Karl Schwede, and Anurag Singh for their multiple readings and helpful suggestions.

References

[1] A. Dress, C. Siebeneicher, *The Burnside ring of profinite groups and the Witt vector construction*, Advances in Mathematics, 70, (1988), 87–132.

[2] J. Graham, *Generalized Witt vectors*, Advances in Mathematics, 99, (1993), 248–263.

[3] S. Glaz, *Commutative Coherent Rings*, Springer-Verlag, New York, 1989.

[4] J. Elliott, *Constructing Witt–Burnside rings*, Advances in Mathematics, 203, (2006), 319–363.

[5] N. Jacobson, *Basic Algebra II*, 2nd ed., W.H. Freeman and Company, San Francisco, 1989.

[6] L.E. Miller, *On the Structure of Witt Vectors attached to pro-p groups*, Ph.D. Thesis, University of Connecticut, 2010.

[7] Y. Oh, *Decomposition of the Witt-Burnside ring and Burnside ring of an abelian profinite group*, Advances in Mathematics, 222, 2, (2009), 485–526.

[8] Y. Oh, *q-deformation of Witt-Burnside rings*, Mathematische Zeitschrift, 257, (2007), 151–191.

[9] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

[10] J.-P. Serre, *Algebraic Groups and Class Fields*, Springer, New York, 1988.

[11] J.-P. Serre, *Trees*, Springer, New York, 1977.

[12] L. Ribes, P. Zalesskii, *Profinite Groups*, Springer-Verlag, New York, 2000.

[13] P. Roberts, *Fontaine rings and local cohomology*, Journal of Algebra, 323, (2010), 2257–2269.

[14] E. Witt, *Zyklische Körper und Algebren der Characteristik p vom Grad p^n*, Journal für Reine und Angewandte Mathematik, 176, 126–140.